NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

INTERNAL CONTROL
IN AN EDI ENVIRONMENT

by

Dal Hyeoung Bae

December, 1991

Thesis Advisor: Myung W. Suh

Approved for public release; distribution is unlimited.

REPORT DOCUMENTATION PAGE

1a REPORT SECURITY CLASSIFICATION Unclassified	1b RESTRICTIVE MARKINGS
2a SECURITY CLASSIFICATION AUTHORITY	3 DISTRIBUTION/AVAILABILITY OF REPORT Approved for public release; distribution is unlimited.
2b DECLASSIFICATION/DOWNGRADING SCHEDULE	
4 PERFORMING ORGANIZATION REPORT NUMBER(S)	5 MONITORING ORGANIZATION REPORT NUMBER(S)
6a NAME OF PERFORMING ORGANIZATION Naval Postgraduate School 6b OFFICE SYMBOL (*If applicable*) 36	7a NAME OF MONITORING ORGANIZATION Naval Postgraduate School
6c ADDRESS (*City, State, and ZIP Code*) Monterey, CA 93943-5000	7b ADDRESS (*City, State, and ZIP Code*) Monterey, CA 93943-5000
8a NAME OF FUNDING/SPONSORING ORGANIZATION 8b OFFICE SYMBOL (*If applicable*)	9 PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
8c ADDRESS (*City, State, and ZIP Code*)	10 SOURCE OF FUNDING NUMBERS Program Element No / Project No / Task No / Work Unit Accession Number

11 TITLE (*Include Security Classification*)
INTERNAL CONTROL IN AN ELECTRONIC DATA INTERCHANGE (EDI) ENVIRONMENT

12 PERSONAL AUTHOR(S) Dal Hyeoung Bae

13a TYPE OF REPORT	13b TIME COVERED	14 DATE OF REPORT (*year, month, day*)	15 PAGE COUNT
Master's Thesis	From To	December 1991	85

16 SUPPLEMENTARY NOTATION
The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

17 COSATI CODES			18 SUBJECT TERMS (*continue on reverse if necessary and identify by block number*)
FIELD	GROUP	SUBGROUP	Internal Control and Electronic Data Interchange

19 ABSTRACT (*continue on reverse if necessary and identify by block number*)

Electronic Data Interchange (EDI) is the electronic transmission of the standard business documents in machine - readable format between parent companies and respective trading partners. As the use of EDI has grown, there have been the associated risks due to an uncontrolled environment. Accordingly, the necessity for effective internal controls in an EDI environment is on the rise. This thesis evaluates and analyzes the feasible internal controls in an EDI environment and provides recommendations for further development. It discusses the basic concepts of EDI, general and application control issues, as well as legal isuues related to an EDI environment.

20 DISTRIBUTION/AVAILABILITY OF ABSTRACT	21 ABSTRACT SECURITY CLASSIFICATION	
☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS REPORT ☐ DTIC USERS	Unclassified	
22a NAME OF RESPONSIBLE INDIVIDUAL Myung W. Suh	22b TELEPHONE (*Include Area code*) (408) 646-2637	22c OFFICE SYMBOL 54Su

DD FORM 1473, 84 MAR 83 APR edition may be used until exhausted
All other editions are obsolete

Approved for public release; distribution is unlimited.

Internal Control
In an EDI Environment

by

Dal Hyeoung Bae
Captain, Republic of Korea Army
B.S., Korea Military Academy, 1984

Submitted in partial fulfillment
of the requirements for the degree of

MASTER OF SCIENCE IN FINANCIAL MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
December 1991

ABSTRACT

Electronic Data Interchange(EDI) is the electronic transmission of standard business documents in machine-readable format between parent companies and respective trading partners. As the use of EDI has grown, there have been the associated risks due to an uncontrolled environment. Accordingly, the necessity for effective internal controls in an EDI environment is on the rise. This thesis evaluates and analyzes the feasible internal controls in an EDI environment and provides recommendations for further development. It discusses the basic concepts of EDI, general control and application control issues, as well as legal issues related to an EDI environment.

TABLE OF CONTENTS

ACKNOWLEDGMENT

It has been a great experience to study financial management at the USNPGS. I wish to express my cordial appreciation to the Korean Army for providing the valuable opportunity to study in the Unites States. I would also like to personally thank Professor Myung W. Suh for his patient guidance, continuous assistance and very thoughtful criticism throughout this thesis. Without his help, my effort would never have been successful. I am also very grateful to Professor Shu S. Liao who carefully read and corrected this thesis. Their expertise and dedication were critical to the completion of this thesis, and a credit to their discipline.

A special thank you goes to my wife, Sun Hee Jang, whose patience and understanding have been most supportive during my study at the Naval Postgraduate School as well as experiencing childbirth during my stay at NPGS. Also my little baby, Jee Hee, whose pure smile has been another great contribution and source of pride. Finally, I am also very grateful to my parents and parents-in-law for their support and patience at home in my country.

I. INTRODUCTION

Electronic data interchange (EDI) is the electronic transmission of standard business documents in machine-readable format between trading partner's computers. Although EDI technology has been in use since the late 1960s, widespread reliance on electronic communication in industry is a relatively recent trend. Because EDI provides a faster, more accurate, less costly method of communication than do traditional methods of business communications, EDI has captured the interest of the global business community. In the automotive, chemical, pharmaceutical, and grocery industries in the U.S., EDI has become a prerequisite for doing business. Growth of EDI into other industries also will be rapid. In addition, several factors, such as wide availability of EDI hardware and software, increasing use of just-in-time system, and so on, stimulate expansion of using EDI.

However, as the use of EDI has grown, so have the associated risks and problems, particularly in an uncontrolled environment. Accordingly, the necessity for effective internal controls in an EDI environment is on the rise. Internal controls are specific procedures established by management to ensure that an entity's transactions are processed completely and accurately, and recorded in accordance with management's authorization. Internal control in an EDI environment requires some change in control process, because EDI is doing more than just changing how businesses communicate; it is changing the way businesses operate and changing industry. Trading relationships are changing, management philosophies are changing, and production techniques are changing. Also, since EDI processes data or documents electronically and all EDI systems are computerized, they have

the same impact as the computer have on the control process, these are, broadly, the concentration and complexity of organization's function. Because of the concentration and complexity in automated systems, the potential for control problems is great. Therefore, there is a need for an internal control to protect an organization from fraud, natural disasters, inadvertent errors, record destruction, and unreasonable transactions.

This thesis intends to evaluate and analyze the feasible internal controls in an EDI environment and provide recommendations for further development. For this purpose, this thesis will start with an overview of EDI in Chapter II, which is a study of the basic EDI architecture and its requirements, the benefits of EDI, EDI standards, and some of EDI applications. The thesis will describe the basics of the internal control issues in an EDI environment in Chapter III. In Chapter IV, general and administrative control issues are discussed, which involve policy and procedures. Application controls which are designed to meet the specific control requirements of each processing application are discussed in Chapter V. Lastly, legal issues related to internal control will be examined in Chapter VI. Conclusions follow in Chapter VII.

II. EDI : AN OVERVIEW

A. WHAT IS EDI?

Electronic data interchange(EDI) is a communication medium which has tremendous practical applications in today's technologically complex business environment. EDI has been described as an electronic transmission of standard business documents in machine-readable format between corporate trading partners' computers and more broadly as an intercompany, computer-to-computer exchange of business information in standard formats. Basically, EDI as a business tool is capable of assisting an organization in attaining their strategic objectives such as reducing paper processing costs, streamlining operations, and achieving a competitive advantage. Yet, the specific benefits of EDI depend on the organizations policy and its environment such as the size of company, associated risks, legal issues, manager's judgement for it, and so on.

Figure 1 illustrates typical EDI transactions in a business environment. As shown in Figure 1, EDI transactions is divided into two categories - internal conduct of EDI and external conduct of EDI. Internal conduct of EDI is the data exchange which is conducted within an EDI company. External conduct of EDI is the data exchange between EDI companies. In this thesis, the discussion will be centered on external conduct of EDI. But most of the discussion will also be applicable to internal conduct of EDI. Electronic funds transfer(EFT) is another type of EDI transaction. Electronic fund transfer refers to the transfer of value electronically from buyer to seller as assisted by financial intermediary, usually a bank.

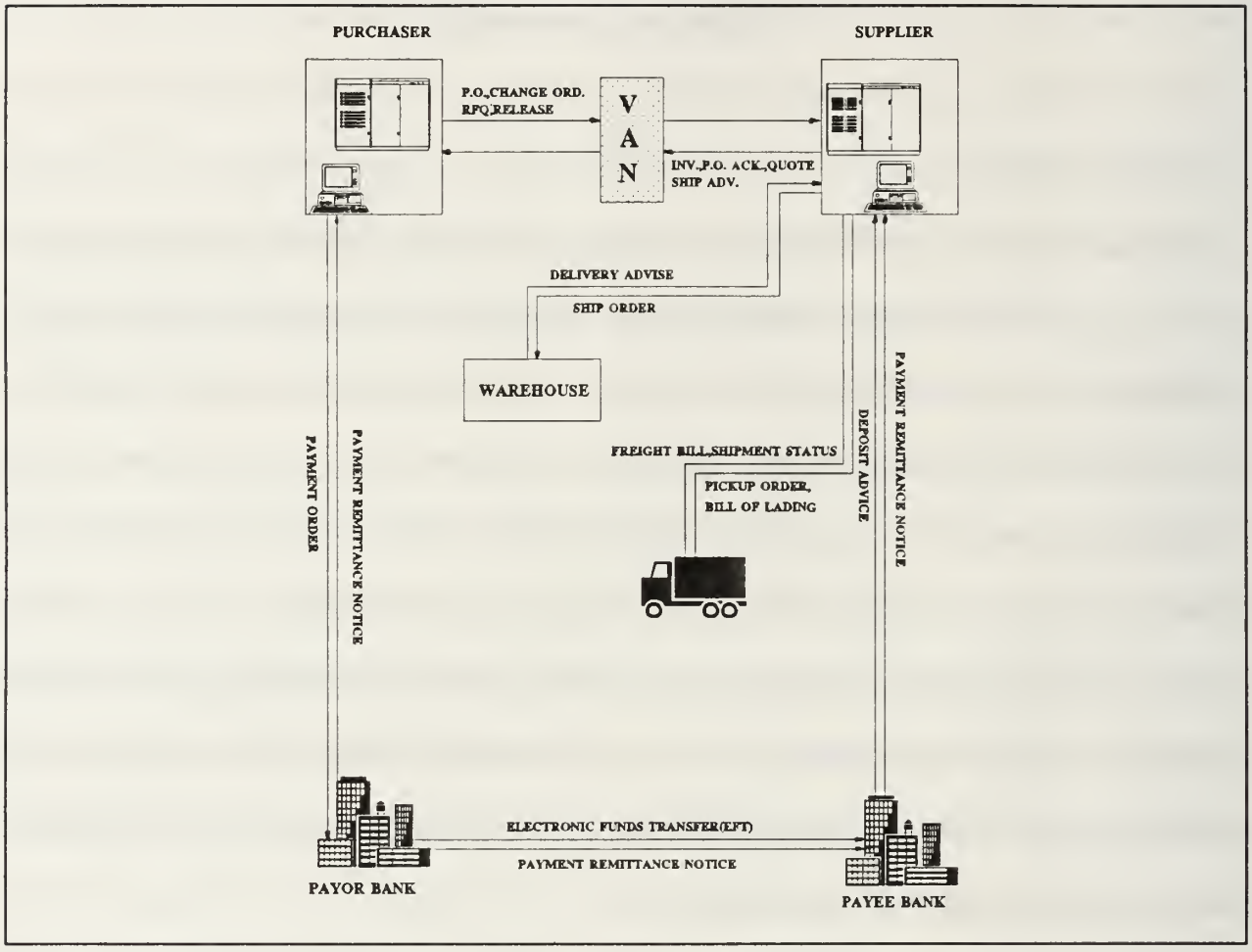

Figure 1 Typical transactions in an EDI system

Figure 2 shows a description of the step-by-step process of EDI.[Ref. 3:p. 67] Typically, the EDI process involves three general functions: communicating with a trading partner, translating data from standard to proprietary format, and directing data to, or gathering it from, an application system, all electronically [Ref. 1:p. 4].

Above all, communicating with a trading partner is the basic process in EDI. EDI requires a combination of technology and management resources to efficiently communicate business information between computers of separate companies. Data transmission is between companies in standard format - that means cooperation between companies is

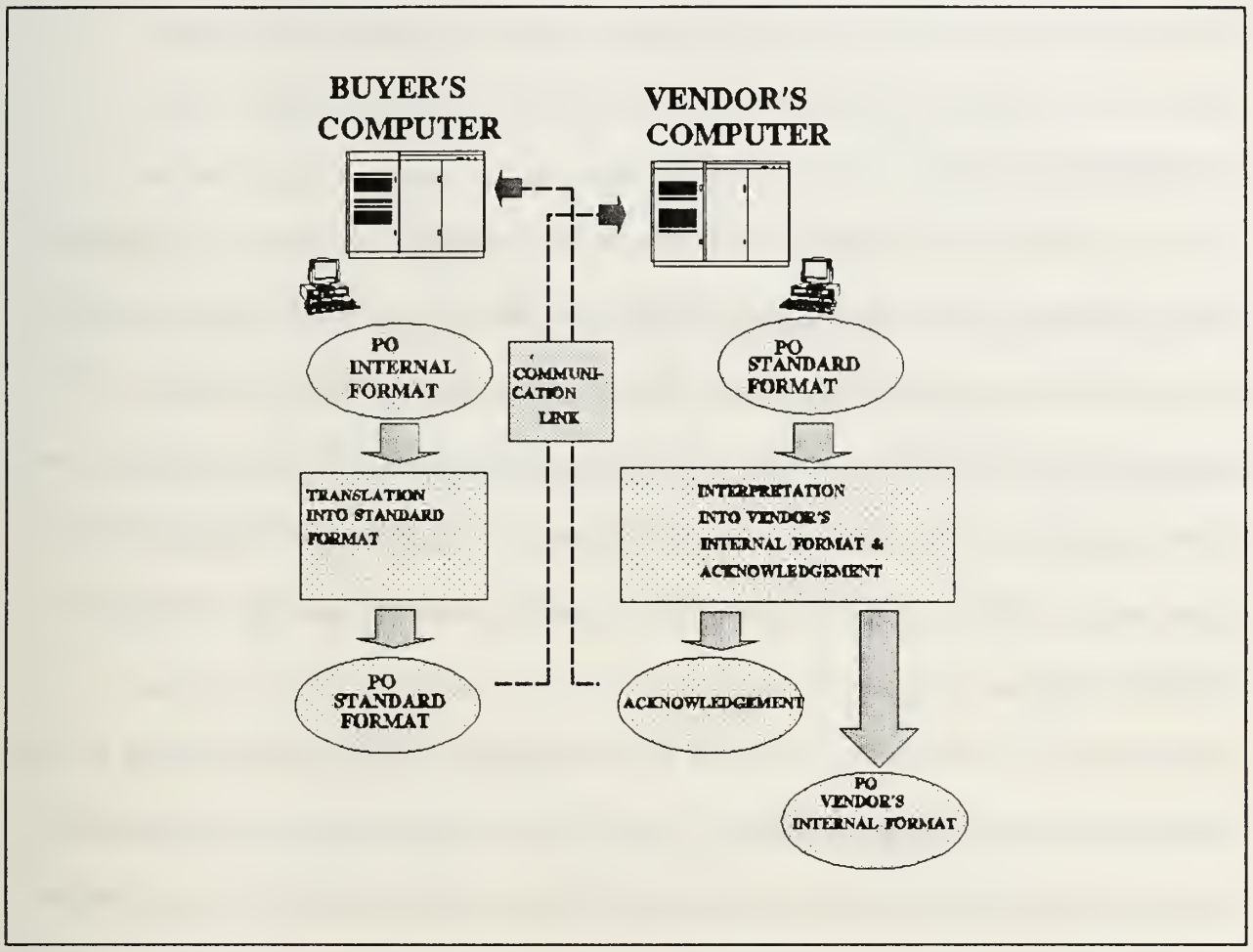

Figure 2 EDI document transmission(example: purchase order)

required to get the EDI system running properly. Ideally, EDI system requires that information flow directly from the sender's application(e.g.,purchasing) to the receiver's application(e.g.,order entry) without human intervention and without paper. Secondary function of processing EDI is translating data from standard to proprietary format. The meaning of the standard data format is that information must be precisely formatted so that a computer can process the information without human assistance. The last function of EDI is a process of directing data, or gathering it from an application system. This function includes control of the data processing function (e.g., how to access, store, retrieve or use

data).

B. BENEFITS OF EDI

From the definition and objective of EDI, one can find the direct benefits of it - savings, accuracy and speed. EDI eliminate paper, postage premiums for overnight delivery, and the like. And EDI communication is direct, instantaneous, and immediately verifiable. That means no more lost or misrouted mail. Documents exchanged are 100 percent accurate and complete. In addition, instantaneous communication is an important EDI benefit to those companies that compete on cycle time. Therefore, EDI is essential in supporting just-in-time(JIT) strategy.

Basically, EDI companies can have the following benefits by using EDI.[Ref. 2:p. 15-19]

- EDI means paperless transactions: Even though most companies use the computer systems, paper-based business processes have slowed the communication, introduced error-prone rekeying of information, added the costs of data entry personnel and postage, and interrupted the flow of information processing. By using an EDI, a company can increase their profitability and efficiency by eliminating costs lazy factors contributing directly or indirectly to administrative lead time, overtime premiums, late or incorrect shipments from suppliers, excess inventories, disruptive production schedules, poor forecasting, and so on.
- EDI reduces costs: EDI contribute to reducing the costs by enabling companies to eliminate some activities and materials, and improve the efficiency of others.
  - Paper: EDI-based, paperless transactions do away with associated costs of

handling and materials to support paper-based communications. A company can reduce handling costs by eliminating manual sorting, matching, filing, reconciling, and mailing. A company can also reduce material costs by decreasing the need for papers and related supplies.

- Inventory: Since reorder requests are transmitted more quickly and accurately than with paper-based system, EDI augments inventory and cycle time reduction program, and make just-in-time(JIT) production and delivery program possible.
- Manufacturing operation: EDI enhances production scheduling accuracy by preventing down time due to late shipments from suppliers. Also suppliers can receive production schedules electronically and feed this information directly into their production control systems.
- Administration: EDI data can provide a thorough audit trail of a company's activity. EDI data may be used as activity reports for management and thereby improving management control of information flow while reducing administration costs significantly.

● EDI improves trading partner relationship: EDI encourages tremendous degree of cooperation between trading partners, because both parties have to cooperate for EDI system to function. For example, many companies in both the manufacturing and service sectors have already adopted EDI to make it easier for customers to order from them, rather than from their competition. For these companies, EDI makes quick delivery, improved order entry, and rapid response to customer inquiry feasible.

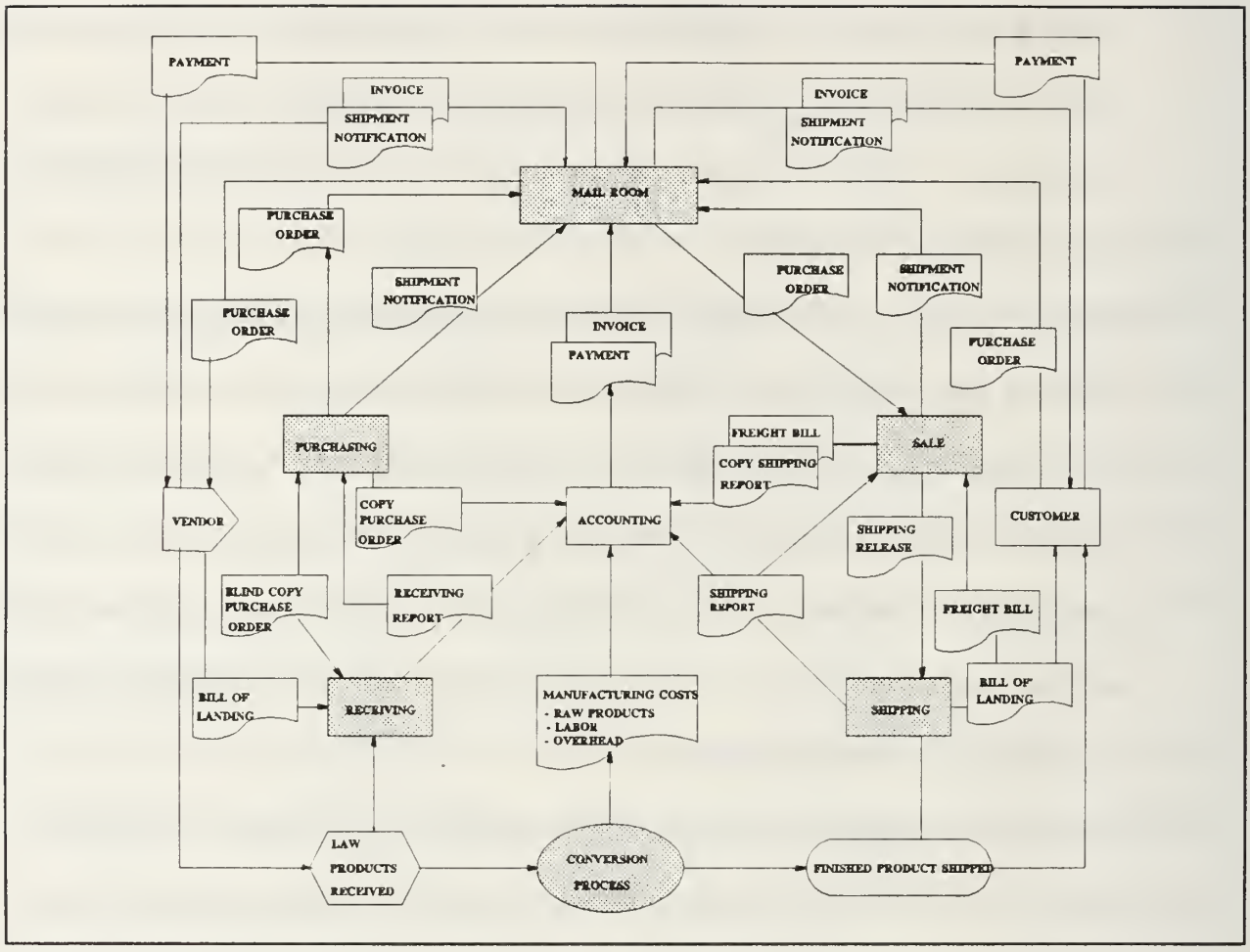

Figure 3 Schematic of paper-based processing system

C. EDI APPLICATIONS

In order to help understanding of control issues in subsequent chapters, this section presents an exemplary model of EDI applications. First, a comparison is made between the paper-based system and the EDI application system not only to find the major difference between these two systems but also to draw on the control issues in EDI application system.

In the paper-based system, most documents, such as purchase order, shipment notification, and invoice, are transmitted to each departments, vendors, or customers by the

function of mail room. For example, a purchasing department buys a variety of materials and services. The purchasing procedure is a very routine activity for the majority of items. The paper flow in a typical purchasing department is established to support this routine, day-to-day activity, yet provides information to a multitude of different individuals in several functional departments. This flow of paper permits the efficient use of purchasing resources in conducting the routine activities of the department and provides needed information to the various departments that are affected by the placement of an order. The manual system provides physical documentation to all these interested parties. Also, the standard flow of documentation is clearly defined. For example, if a purchase order has an exact number of copies, the distribution of each is specified. The reason for this standardization of procedures is that the multitude of clerks supporting the system can process the documentation with minimum effort and uncertainty. Besides, the flow of documentation permits managerial discretion. If certain conditions that are not routine or normal arise, responsible managers can take corrective action before any problems arise. Figure 3 shows an example of the paper-based transactions and the flow of paper, which shows the procedure to accomplish above objectives.[Ref. 5: p. 9]

However, the paper-based process requires a lot of lead time, large quantities of paper documents to be moved from and to various locations within and outside the firm. Even though the firm's internal work is computerized (not an EDI application), it is costly and illogical to have its computer spit out paper documents that are mailed to another company that rekeys these documents into another computerized system.

In order to convert from a paper-based system to an EDI application system, there are

several issues that need to be addressed.

- To eliminate human intervention, it needs to process the entire set of internal, external transactions electronically. It includes the business cycle of ordering, receiving, stocking, paying, selling, shipping, billing and collection.
- It must be able to translate conventional paper-based documents into the ANSI X12 standard, which is a cross-industry, cross-functional EDI standard.
- It must facilitate coordination of the efforts among all participants.
- It must be complemented with EFT for automatic, same-day payment and collection.
- It must support online query of ordering, shipping, inventory, payments, collections and cash flow status and must interface with bar-code scanners to facilitate fast movement of products through operations.
- It needs to generate flash reports on expectations and coming events.
- It must generate management reports that show transportation performance, order activity and trends.

There are different ways of achieving EDI, such as courier service alternative, third-party service alternative, and direct computer-to-computer alternative. Figure 4 illustrates each of these alternatives. [Ref. 5: p. 11]

The courier EDI design alternative provides overnight delivery of magnetic tape or disk and is the easiest and simplest to develop and implement. The use of tape or disk can help reduce errors, but it still requires a great deal of manual intervention.

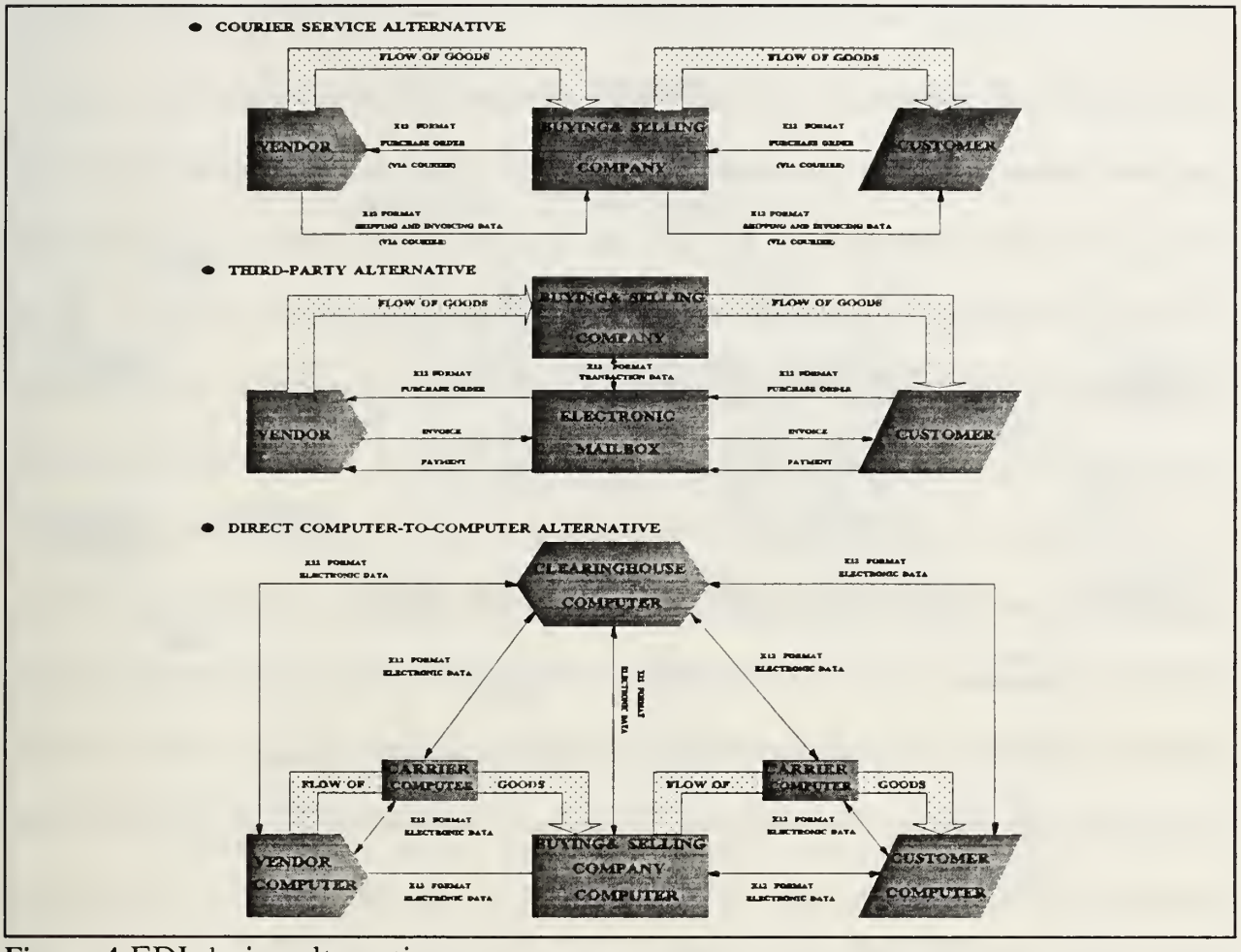

Figure 4 EDI design alternatives

The third-party service EDI design alternative enables a sender to transmit data in EDI format to an electronic mailbox and a receiver to access the mailbox at their discretion. This approach simplifies telecommunication issues such as line speeds and protocols between multiple users. Other issues such as multi-destinations and times of the day don't have to be considered. Users simply dial in and drop off their mailbag, then network distributes the enclosed documents to the trading partners' mailboxes. The trading partners dial in to pick up their documents, usually the same day.

The direct computer-to-computer linkage between all parties is the ultimate EDI goal.

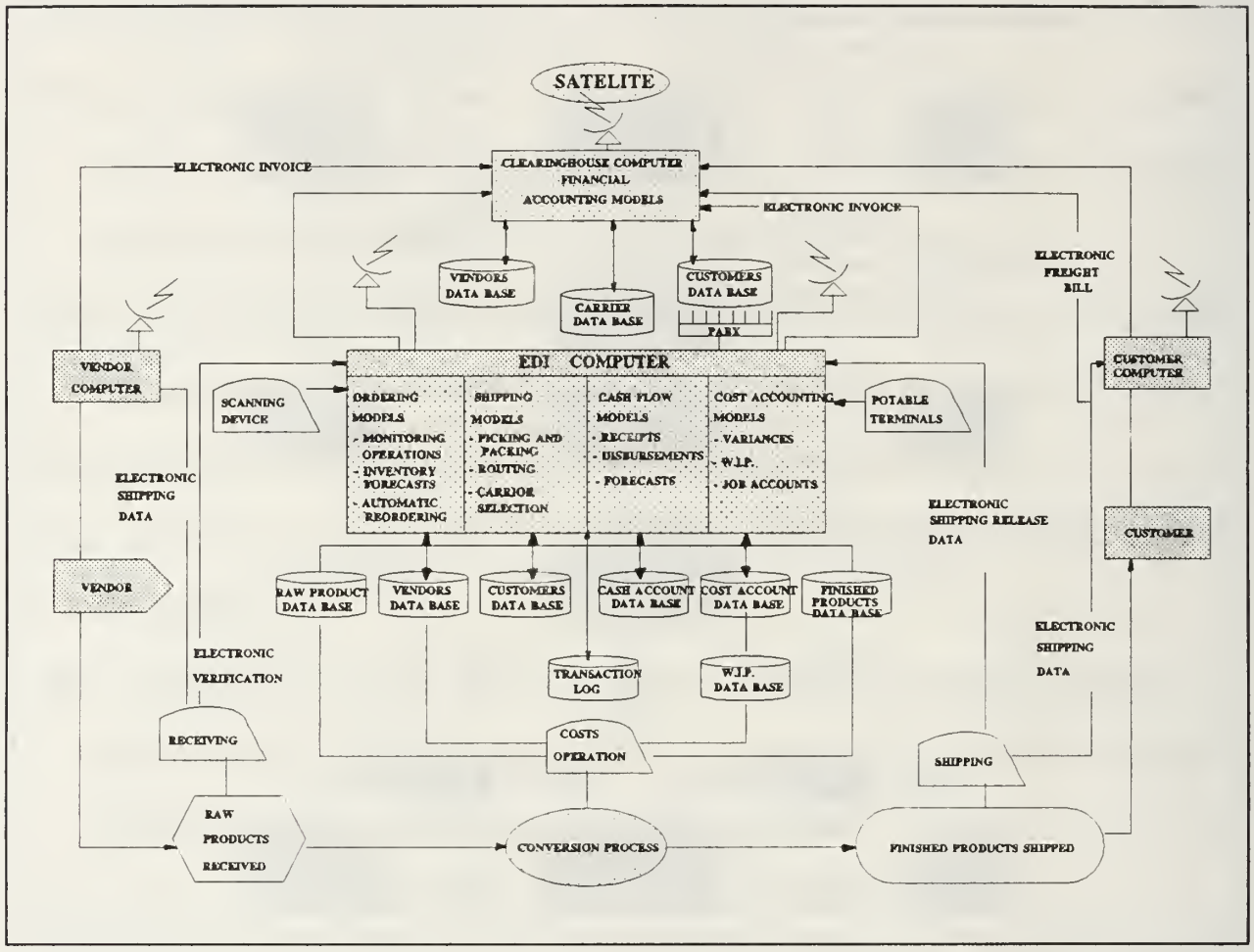

Figure 5 Technology platform for the EDI computer-to-computer system

This links take advantage of electronic communication speed and accuracy. A clearinghouse component such as a full-service bank can reduce significantly the bookkeeping functions for all participants. Clearinghouses with expertise in EDI can handle freight bills and invoices, audit these payments, protect against duplicate payments, and reformat data and transmit it directly to subscriber's computers for reconciliation and management reports.

Before developing and implementing EDI, a company should carry out a thorough cost/benefit analysis to identify EDI opportunities and problems, and then develop a pilot program. This preliminary process is to make sure that EDI is implemented with maximum

effectiveness and efficiency.

Figure 5 illustrates a detailed design for direct computer-to-computer EDI applications. The major components of the proposed EDI network in this example are one geosynchronous business communications satellite for relay between all parties, earth stations for access and transmission of signals, stations for satellite tracking and telemetry, fiber optic links, muxes, private automatic branch exchanges(PABXs), and the traditional telephone system. Bar-code scanners are also required in this direct computer-to-computer EDI system, because all items in this company's inventory will use a bar code for identification and for product movement on computerized conveyor belts. As an item moves along the belt, it will be scanned automatically, identified and routed to the correct spur of conveyor, where it is unloaded for production, loaded for shipment or placed in storage. Preliminary tests and benchmarks show that this new system will reduce the average time to process an item from three hours to five minutes. Several portable terminals have an important role in this new system. Inventory taking and verifying will be handled by terminals hung from workers' belts. A laser-wand attachment reads the product identification bar code of every item in inventory. The terminals store in nonvolatile memory data that are uploaded to the main processor through fiber optics. They have complete access to product information from the main data base, which can help close a sale. The sales representative, sitting in a customer's office, can access a variety of models, ranging from engineering specifications and design aids to economic analysis. Upon making the sale, the sales representative immediately transmits the sales data to the company's mainframe to begin order processing.

Flash reports are generated automatically by the system. Example of flash reports include receiving orders, shipping orders and rejected customer orders. Also, receiving and warehouse personnel receive shipping notification as to when products will arrive and by what carrier.[Ref. 5:p. 12]

D. EDI ARCHITECTURE AND ITS REQUIREMENTS

1. EDI architecture

In order to facilitate the upcoming discussion of controls, it is helpful to group EDI transaction processing into three major functions. As shown in Figure 2 and the description of the basic process of EDI, there exists three major functions: the communications interface, the EDI interface, and the application system. These functions comprise the EDI architecture and are generic in that they are not dependent on any specific hardware, software, communications protocol, or processing environment. Figure 6 illustrates the architecture on both ends of a communication link.[Ref. 1: p. 12-13]

- Communication interface: Transmits or receives the electronic document through the communications network. The communications interface has controls to ensure the data is received properly, especially in the event of transmission error or interruption. In addition, routing verification and acknowledgement procedures ensure the destination is valid and the system is authorized to send or receive data. Additional control techniques are performed by hardware and system software and, typically, are time-tested by companies' normal teleprocessing procedures.
- EDI interface: This function is divided into two areas - the EDI translator and the

application interface. The EDI translator translates between the standard format and the trading partners' proprietary format. It can generate functional acknowledgements for functional groups of transactions received from an EDI partner. Subsequent matches help to ensure that all transactions sent were received and visa versa. The EDI translator can also perform authorization checks of transactions received against a trading partner master file to verify the partner and its authorized transactions.

- Application interface: The application interface moves electronic transactions to or from the appropriate application system. This entails either distributing inbound transactions to appropriate systems, or collecting outbound transactions from those systems. Inbound transactions, once passed to the application system, are processed by the application system, and subject to the same controls as other transactions not received via EDI.

Figure 6 also illustrates the flow of an inbound transaction through the EDI architecture and distribution by the application interface to several application systems. The diagram would be reversed for an outbound transaction, with the application interface collecting from the application systems.

2. Data structure

In order to know how to transmit the document in EDI system, we need to search for data structure. Generally, each electronic document is considered a single EDI transaction. Transmission headers distinguish between document types, such as purchase orders or invoices. Therefore, a variety of documents can be sent together in a single transmission. The data included in each transaction set conveys the same information as a

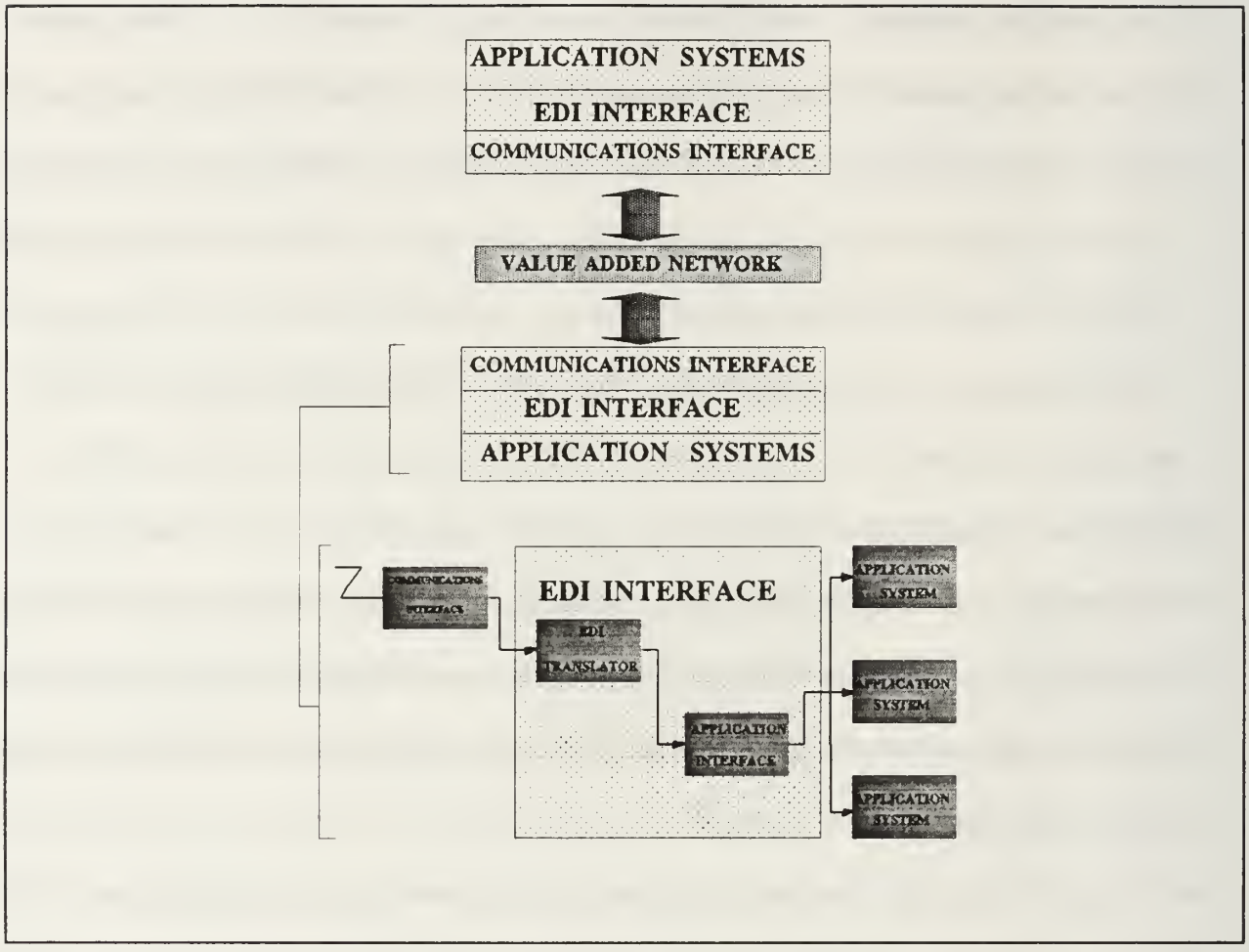

Figure 6 Data structure of an EDI transaction

conventional printed document, and is divided into three corresponding areas.

The "header area" contains information that pertains to the entire document, such as date, company name and address, and P.O. number. The body of the document is the "line item area." It contains the actual business transaction data on quantities, item description, and unit prices. Finally, the "summary area" that may contain transaction totals and shipping information.

Header and trailer record surround the transaction set and allow several electronic documents to be sent together. Multiple transaction sets can be sent to a trading partner in

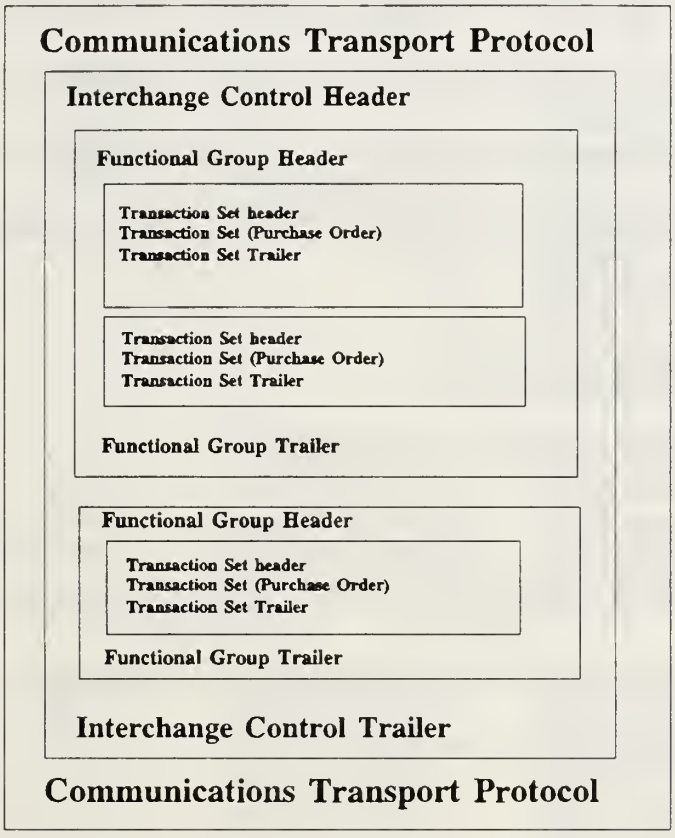

Figure 7 Data structure of an EDI transaction

the same transmission by grouping similar transactions into functional groups that differentiate invoices from purchase orders, for example. Functional groups are surrounded by functional group headers and trailers. When several functional groups are sent in a single transmission, those groups are enclosed between an interchange control header and the trailer. Finally the entire interchange is surrounded by communication transport protocol layer that contains control and exchange information necessary in the communications link. Figure 7 illustrates the data structure in the transmission of multiple transaction sets.[Ref 1: p. 8]

3. Hardware / software requirement

For EDI system hardware, there exist three basic options: mainframe only, microcomputer only and microcomputer as a front-end processor to a mainframe. If one includes the third-party support as an option, there are four different system approaches regarding the hardware platform for EDI, as illustrated in Figure 8:

- PC based configuration
- Mainframe based configuration
- PC-to-mainframe configuration
- Third-party support.

The best computer configuration can be different, according to user's environment, and each configuration has its own advantages and disadvantages. Figure 8 depicts the merits and demerits of each.[Ref. 3:p. 69]

EDI software consists of computer instructions that translate information from unstructured, company-specific format to the structured EDI format and then communicate the EDI message. EDI software also performs this activity in reverse (receives the message and translates from standard format to company-specific format). EDI software can be developed in-house or it can be purchased from commercial software vendors. EDI can be performed on various types of computers and EDI software is currently available for mainframe computers, minicomputers, or microcomputers. The major function that EDI software performs is formatting or translation. Formatting software generally uses a table structure to perform the translation. The software includes tables consisting of the standard

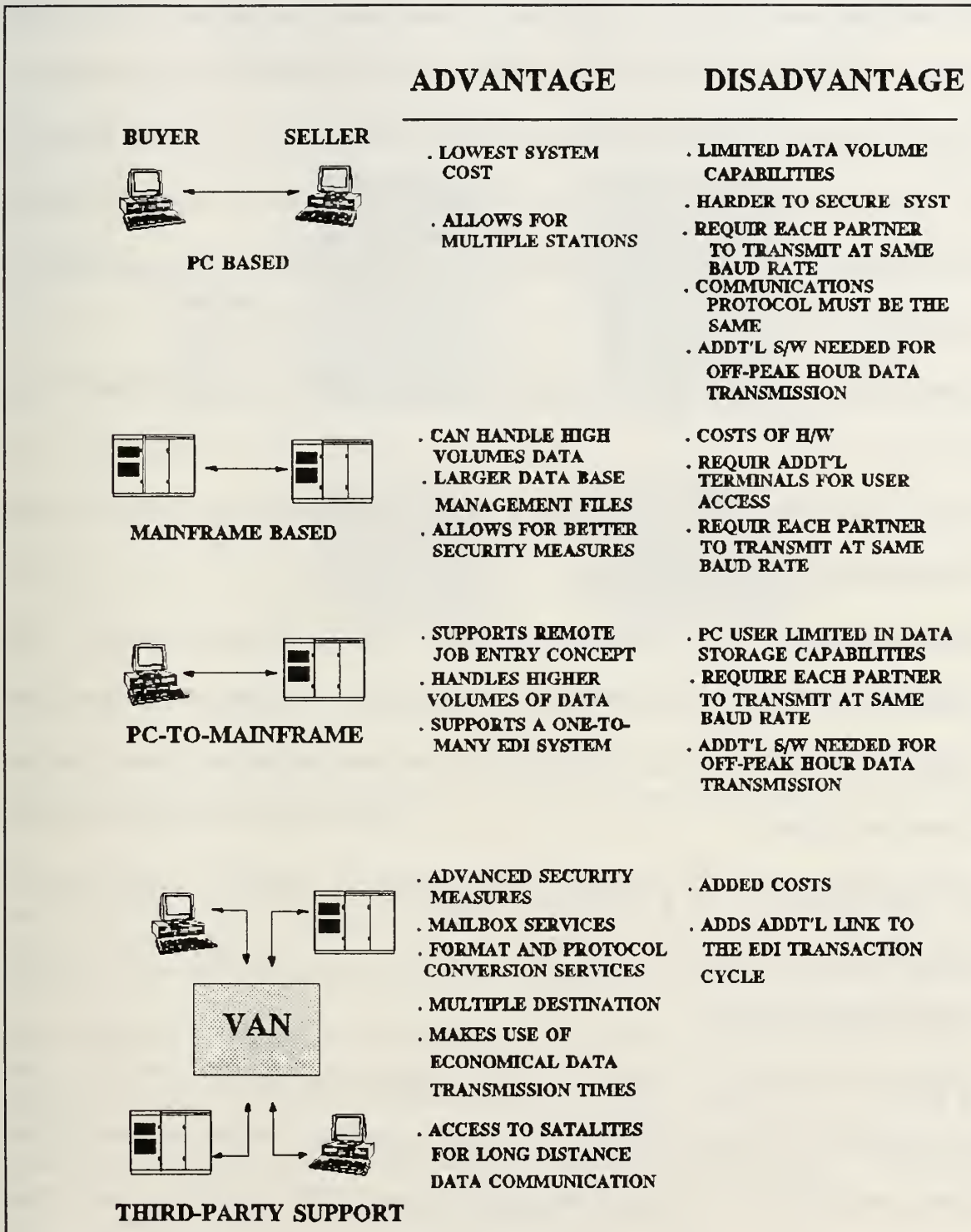

Figure 8 Hard platform for EDI

data dictionary and syntax rules for the data segments and elements of a given EDI transaction set. The actual transmission of the EDI message is controlled by communications software. This software manages and maintains the phone numbers of trading partners, performs automatic dialing, and also produces an activity log. Figure 9 shows the normal sequence of activities performed by EDI software for both incoming and outgoing EDI. [Ref. 4: p. 92]

There are a number of software categories associated with an EDI system. These include:

- Data management software: Designed to systemically organize data into files for easy access, retrieval and update.
- Format/conversion or . translation software: User information input into transaction format and then converted to the electronic transmission protocol. Also capable of converting transmitted data from the communications protocol to the transaction format.
- Communication software: Controls the data being transmitted via phone lines to and from EDI partner.[Ref. 4: p. 66]

4. Communication options

Various options exist to establish an EDI communications link. The two most prevalent methods are a direct connection to the trading partner's system and the use of a value added network(VAN). As more companies engage in EDI partnership, each often using different systems and formats, the effort to transmit and process EDI transactions becomes increasingly difficult and costly. A variety of hardware, software, and

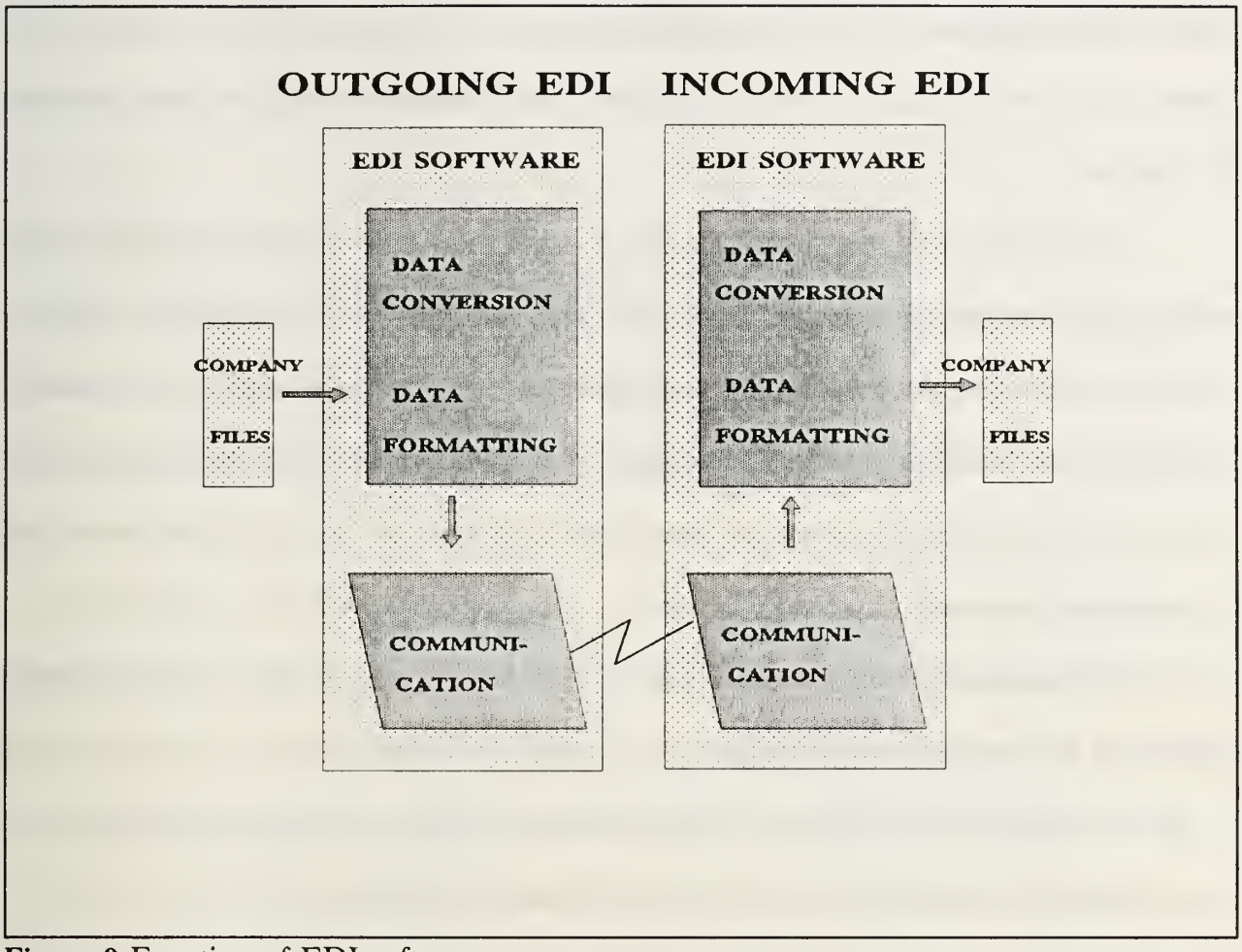

Figure 9 Function of EDI software

communications options may be required to maintain EDI relationships with numerous partners. Value added networks(VANs) are being used by many companies to address these considerations. VANs are third-party networks that store and forward EDI documents for trading partners. The external conduct of EDI in Figure 1 represents a trading partner's simplified requirements to maintain an EDI relationship when using a VAN. Essentially, only the partner and the VAN need to have compatibility.

Typically, the sending partner links electronically with the VAN and transmits documents. Upon receipt, the VAN determines the recipients and places their respective

documents in a file on the VAN's computer system - an "electronic mailbox" - where they remain until each recipient connects with the VAN, accesses its file, and retrieves the documents.

VANs can minimize compatibility issues, since most have the facilities to deal with many types of communications hardware, software, and protocols. They also can alleviate scheduling problems, since the sender and receiver need not communicate simultaneously. In addition, the "mailbox" facility enables one trading partner to easily deal with multiple partners in connection. However, as always with a third-party, assurance of a controlled environment is essential.

VANs may perform other processing services in addition to storing and forwarding. In general, services by VANs include:

- Store and forward services in which mailbox facilities are established to store inbound transactions for retrieval by the intended recipient.
- Compliance checking services to determine if transactions are formatted in the standard agreed to by the trading partners.
- Translation/conversion services to translate incoming transactions into the format agreed to by trading partners.
- Interconnection services to allow customers to deal with trading partners that use other networks. Since all partners may not use the same network, gateways to other networks should be available. [Ref. 1: p. 5]

There are cost considerations as well. Typically, VANs charge both trading partners to receive and deliver transactions. Processing services, such as compliance checking and

interconnection with other networks, are usually additional. The costs vary depending on the network, volume of transactions, and services used.

E. STANDARDS FOR EDI

EDI standards provide a widely accepted format to convey the meaning of the exchanged data. This allows a sender to encode data in the same format for many receivers, and requires the receiver to maintain only one piece of software to decode data received from many senders.

The exchange of electronic documents between companies in standard data format is critical for EDI. Only by using strict EDI standards can computers transfer and process information automatically. For EDI, there are two standards issue that must be addressed: communication standards and document contents standards. [Ref. 2: p. 20-22]

- Communication standards (protocol): Standardize the language the computer use to communicate with each other. As a company increases the number of its EDI trading partners, it is inevitable that some new trading partner will use an incompatible protocol. To resolve this issue, many companies use an EDI network service as the communications intermediary between them and their EDI trading partners. The line speed between communicating computers also should be standardized. In order for computers to understand one another, they must send and receive data at the same rate. the difference in data rate can be resolved by EDI network services.
- Document content standards: Standardize the order in which information is to be

Translation of Purchase Order for
Electronic Business Data Interchange

Appendix
Format for EBDI

Related Purchase Order Section

ST*850*8400 N/L

Purchase Order

BEG*00*SA*5KK3-05530***840423 N/L

Date: 04/23/84 — 5KK3-05530
This Number Must Appear on all Boxes, Packages, Shipping Documents & Invoices.

N1*SE*92*400061 N/L

To: Selling Party 400061
123 E. West St.
Anytown, USA 99999

N1*BY**91*162 N/L
PEP*SD*Joan Buyes N/L

From: Buying Party 162
444 W. East Ave.
Downtown, USA 99999

N1*ST**91*1100 N/L

Buyer Contact
Joan Buyes

ITD*01*03*2**20 N/L

SHH*SD*010*840513 N/L
SHH*DD*002*840515 N/L

Ship: Ship To Party 1100
Receiving Dock
100 Main St.
Downtown, USA 99999

FOB*PP*M1*Less C/L FA N/L

TD2*O*E N/L

PO1*1*48*CT*56 75*QT*IN*1147560*VN*20784 N/L
SCH*16*CT****002*840515 N/L

Terms
2/20LCC

SCH*16*CT****002*840522 N/L
SCH*16*CT****002*840529 N/L

Ship Date	Due Date
05/13/84	05/15/84

PO1*2*16*CT*59 5*QT*IN*1124486*VN*14096 N/L
PO1*3*16*CT*46*QT*IN*1107820*VN*51193 N/L

FOB	Freight Allowance
Mill	Less C/L FA

CTT*3*80 N/L
SE*19*8400 N/L

Ship
Truck

Line No.	Your Item No.	Our Item No.	Item Description	Unit Price	Quantity	UOM	Item Due Date
1	20784	1147560	23x35 8100 Shasta	56.75	16	Ctn	05/15/84
			Gl Bk Whte		16	Ctn	05/22/84
					16	Ctn	05/29/84
2	14096	1124486	23x35 880 Shasta	59.50	16	Ctn	
			Suede Bk Wh				
3	51193	1107820	23/35 Offset Opaq	46.00	16	Ctn	
			Vellum				

Figure 10 Example of EDI standard document

sent and received to help the receiving computer to process the information. Enabling computers to process the data received without human intervention is the role of document content standards. Document content standards fix the order in which data appears within a given document. Both trading partners must agree on the precise format and design their computer programs to expect document data to be sent/received in that format. Hence, the receiving computer will be able to retrieve information, and order quantity, from the data received. Document standards are the essence of EDI: When referring to document content standard, most people just say "EDI standards".

American National Standards institute(ANSI) has made a significant contribution to the development of standard EDI transactions across industry lines. It develops standards based on the agreement of all groups concerned. ANSI also provides information on foreign standards and represents the United States' interests in international standardization work. ANSI membership consists of industrial firms, trade associations, technical societies, labor organizations, consumer organizations, and government agencies. ANSI X12 published by ANSI contains the most inclusive set of standards in an EDI environment. Figure 10 shows an example of a purchase order document that conforms to the requirements of ANSI X12.[Ref. 3: p. 54]

III. CONTROLS IN AN EDI ENVIRONMENT

In the previous chapter, EDI was introduced and discussed, providing an overview of the process involved and of future applications. EDI promises significant cost savings and productivity gains for business operations. However, EDI will require a rethinking of how basic controls are implemented because traditional internal control principles and techniques may not be valid for EDI systems. In Chapters III, IV, V, and VI, these internal control issues will be discussed as they pertain to an EDI environment.

A company's use of EDI can have a significant effect on internal control activities, as shown in Table 1. [Ref. 2:p. 44] Therefore most of EDI companies have a lot of concerns about internal control issues because, even though EDI companies gain advantages from using EDI systems, converting to the EDI requires different internal controls that are more complicated and elaborate than those of a manual system. There are several reasons why internal controls are important in automated systems. Above all, there is a growing reliance by management on computer-generated reports: the accuracy and reliability of such reports are a function of controls in an EDI environment. Also, as increasing amount of resources are being allocated to computerized activities, a good control process is necessary to make sure that the resources are used effectively. Another reason is that the risk caused by control problems is greater in a computerized system, and indeed, there is much evidence of poor controls in companies today. For example, the result of recent studies indicates program fraud, record destruction, file security problems, and operating inefficiencies due to inadequate controls. [Ref. 7:p. 64] Lastly, it is also a reason that management has new

Control Concerns	Effect of EDI
Order/ payment control : insuring only authorized sources can place orders and initiate payments.	• No authorization "sign-off." • Less human intervention means less control.
Audit trail of activity : tracking data flow within the company and recording authorizations.	• Computerized data changes information security procedures. • Lack of paper includes paper backup files. • EDI data flow can be documented internally, between company and EDI VAN, and between company and trading partner.
Payment validation : Reconciliation of invoice, purchase order, and receiving documents to assure correct payment amount.	• All of these documents are now computerized. Lack of paper changes the validation process.
Correspondence of accounting records with actual transactions : Insuring that internal company data reflects actual inventory and dollar figures.	• All files are computerized ; no paper backup to verify records.

Table 1 EDI effects on internal controls

responsibilities for the effective design and implementation of an internal control system.

Therefore, internal control should be conducted in accordance with this electronic environment. Controls in an electronic environment need to be restructured from those typical of manual systems to those that will complement the characteristics of the computer. In an electronic system which does not depend upon documents to capture information about transactions, internal controls must be modified to provide assurance that all transactions are properly processed.

However, the objectives of internal control, which are to safeguard assets and to provide

reliable data, remains the same. Certain basic characteristics of the organization are essential in ensuring that these objectives are achieved. Though these organizational elements on the surface may look the same, those required for an EDI system may take on a slightly different form. These organizational issues might include competent personnel, segregation of functions, proper authorization of transactions, documentary evidence that transactions are executed as authorized, appropriate recording of transactions, security problems, periodic comparison of records with assets, and so on. These issues will discussed in the following three chapters in detail.

Generally, internal controls are divided into two categories: general and administrative controls and application controls. [Ref. 1:p. 15] General and administrative control are intended to ensure proper implementation, maintenance, and continued operation of programmed procedures, security of data files and programs, and appropriate division of duties and responsibilities. In short, general controls provide the standards and guidelines for a variety of applications. Application controls are designed to meet the specific control requirements of each processing application. Application controls are those computerized and manual procedures that are integral to an application system's processing and ensure only complete, accurate, and valid data is entered and processed. They also provide assurance that data is maintained properly, and that processing results meet management's expectations. The main difference between these two controls is that application controls are data-oriented and specific task-oriented, and general controls are procedure-oriented on the whole. Figure 11 shows the relationship between general control and application control with three example applications.[Ref. 8:p. 519]

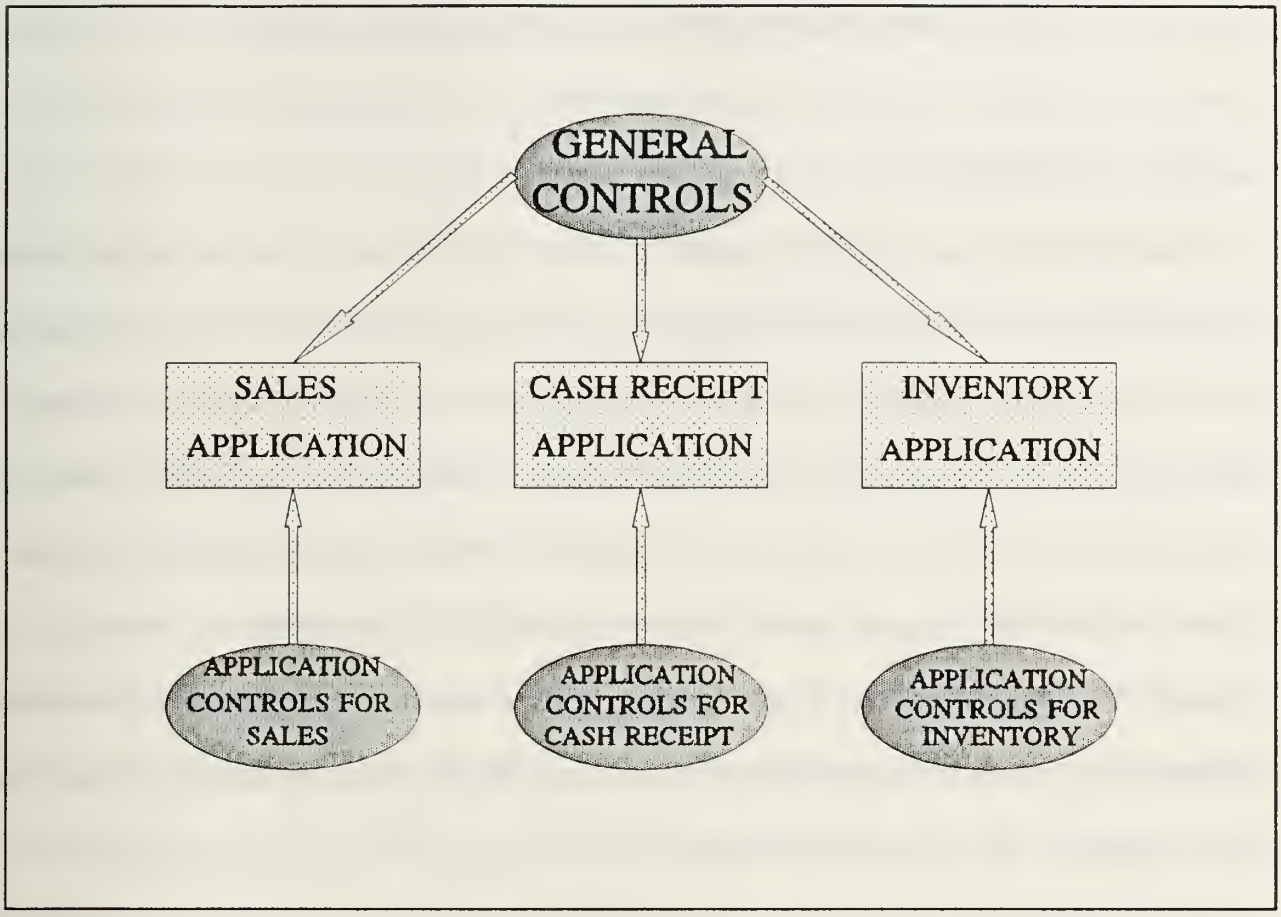

Figure 11 Relationship of internal controls

The focus of this thesis is on internal control issues, specifically, general controls and application controls in an EDI environment. In order to facilitate the study of internal controls as they apply to an EDI environment, the primary internal control issues will be discussed and presented separately in the subsequent three chapters of this thesis. Chapter IV will address general and administrative controls. Application controls will be discussed in Chapter V. Finally, Chapter VI will investigate potential legal issues regarding internal controls as they pertain to internal controls in an EDI environment.

IV. ADMINISTRATIVE AND GENERAL CONTROL

A. INTRODUCTION

Administrative and general controls are procedures used within the electronic environment to ensure effective development and continued operation of these programmed procedures. In short, general controls cover the organization, implementation, maintenance, and security of packaged systems and system software. Usually, general controls encompass all application systems that operate within a given MIS environment. The control procedures in place within MIS typically remain the same when EDI is introduced into environment, although EDI may raise new issues in each general control area. However, if an EDI department is created independently of an existing MIS function, separate general control procedures must be established and maintained.

This chapter will address organizational controls, operational controls and documentation, backup and disaster plans, and an audit trail developed for use in an EDI environment.

B. ORGANIZATIONAL CONTROLS

The main issue of organizational controls is functional segregation of duties. Segregation of functions is required so that no single individual is in a position to perpetrate and conceal an error or irregularity. Generally, the division of functional responsibilities should provide for a separation among the functions of initiation and authorization of a transaction, the recording of the transaction, and the custody of the resultant asset. Such a division of

responsibilities, in addition to safeguarding assets, provides for the efficiencies derived from specialization, make possible a cross-check that promotes accuracy without duplication or wasted effort, and enhances the effectiveness of a management control system. In a control standpoint, automation has had a great effect on organization structures. As a result of automation, as discussed briefly in the previous chapter, there has been increased centralization of data processing activities and the concentration of data processing functions. Therefore, the importance of the role of functional segregation is increasing under automation data processing such as EDI systems.

Before the advent of computerized systems, most of the individual operating departments usually did their own clerical paper work. But, now, data processing center tightens coordination and helps eliminate duplicate demands by processing data and generating reports that provide operating department with the bases for carrying on their individual activities. Data can be transmitted from the source, possibly a remote warehouse or trading partners' computer, to another point for processing: the results of processing are then returned in the desired format to the applicable locations. Such systems are justified on the grounds that the time and costs associated with processing data are reduced and, accordingly, management has more timely information on which to control company operations effectively.

However, the centralization of data processing activities has resulted in the concentration of many processing steps into one department and the concentration of traditional accounting data along with operating data. Such concentration is commonly referred to as integration, in which related elements of different data processing activities

are combined into common and coordinated procedures and a logical work flow. In this current organizational environment, the centralization of data processing into one department emphasizes the importance of proper control of the data processing center itself. The segregation of duties becomes critical in an automated environment because of the concentration of functions, personnel and data in a centralized location.

In many data processing systems the applications being designed today are equipped with programmed decision rules combined with machine-readable files which create the impression that the authorization and recordkeeping functions have been merged. In this kind of system, the authorization function originates with operating personnel. In order to provide the replenishment decision rules within the stored computer program, the system designer and programmer would interact with purchasing people who have knowledge of the inventory items, usage history, and vendor history. Therefore, the authorization to replenish inventory originates with the operating people and is passed along to systems designers and programmers, who program the parameters to be included in inventory replenishment decisions. Normally the recordkeeping in automated systems is done by computer operation personnel, who handle the inventory files in machine-readable form. The custody of the assets acquired through inventory replenishment decisions would still be the responsibility of warehouse personnel.

In order to ensure the continued integrity of the system, it is necessary to separate the system's planning and programming function, the operations function, and the program maintenance and data library function. This segregation will serve to maintain the following: [Ref. 7:p. 80]

- It provides an effective cross-check of the accuracy and propriety of changes introduced into the systems.
- It prevents operating personnel from implementing revisions without prior approval and thorough checking.
- It eliminates access to the equipment by non-operating personnel and other people who have knowledge of the system.
- It improves efficiency because the capabilities, training, and skills required in carrying out these activities differ greatly.

C. OPERATIONAL CONTROLS

As aforementioned, general controls include control over the implementation and maintenance of programmed procedures, computer operations, computer and communication security, and configuration management. Operational controls encompass above issues.

1. Implementation and maintenance control

Implementation controls are designed to ensure the appropriate development, testing, and implementation of a system. Maintenance controls ensure that EDI programs are designed, implemented, and maintained properly. Typically, an EDI system will be implemented or modified in accordance with the methodology used for operational and financial application systems.

An EDI system, specifically the translation and interface software, must be maintained properly to remain effective. For example, it is imperative that new or the most

current revisions of EDI standards are used and that all required versions are available to all trading partners that use them. In addition to standard change management over software and hardware, the EDI trading partner and VAN relationships must be maintained. Failure to add the new and delete the old can increase the risk of unauthorized transmission, based on an invalid trading partner agreement. Also, it may delay the processing of a newly acquired partner's transactions.

2. Controls of computer operations

EDI is a computerized system. Thus controls are also required in the computer operations. One of the implications of this is that EDI requires elaborate controls for ensuring that processing can be resumed properly in the event of a failure. That is, there must be some mechanisms to ensure that procedures exist for the resumption of processing in the event of failure or stoppage during any phase of EDI. Techniques for achieving this objective include establishing a number of strictly enforced procedures for job scheduling, setup, and running, backup and recovery, and failure and abnormality reports. During the communications interface, those procedures must address transmission error correction, re-transmission, and receipt.

Another implication of computerized operation is that its input process is different from manual systems. In an EDI system, edit checks are primarily placed in programs that accept transaction input from the terminal user and from the trading partner. Program logic can be designed to substitute for human judgement, but with much greater reliability. In this way, data can be subjected to more types of edit checks and more consistent editing than when processed by humans. Its shortcoming is that unanticipated transactions may not be

properly processed by the programs. The human processor are more flexible in this area in that he possesses judgement and intuition which permit proper handling of exceptional transactions.

3. Controls of computer and communication security

The security of data files and programs is a major issue in EDI. A security development procedure must address the areas of importance for EDI users from the point of initial data input through data transmission to data receipt by the trading partner. Security issues involving EDI should be viewed as an extension of current security issues, procedures, and standards which many organizations have already addressed with other computerized systems. And through prevention and detection, security controls should ensure that unauthorized changes are not made to transmission data, data files, and programs.

The higher security risks in EDI than in manual system are due to the fact that personnel external to the organization such as suppliers, other trading partners, and third parties(VANs) can have access to sensitive data. Vital information concerning pricing, contracts, quotes, and purchase orders are routinely transmitted electronically in the EDI environment. It is imperative that this information be secured and accessed by only authorized parties. An issue not exclusive to EDI, but common in the use of VANs, is the security of data while it resides with a third party and when it is transmitted on their network. If a VAN is used, then the company must be concerned about the control environment of that service. Since sensitive information is being routed through the VAN, a weakness in control at the VAN site can affect the confidentiality and reliability of

information. Contractual agreements with the network should specify required controls and provide for a verification process which could be performed by internal or external auditors. An assessment or third-party review of their data file and program security, and other general controls, can ensure that a VAN meets an organization's control objectives.

The protection of the data base and maintaining the integrity of the data transmitted are the goals of the security system. Protective security measures are built into each of three security elements. These elements are: [Ref. 3:p. 48]

- Physical : Security measures that restrict physical access to the system. For example, locked doors, keys, guards, alarms, etc.
- Procedures : Security measures that provide controls over authorization to see or use information. For example, authorized employees' lists, information elements access approval, passwords, and separation of duties.
- Logical : Security measures that restrict access to information in electronic forms. For example, software which implements access control through the use of fingerprint recognition, voice recognition, and cryptography. There are two cryptographic mechanisms that are essential for EDI systems. These are encryption for ensuring data confidentiality and authentication for ensuring data integrity. Encryption is the process of converting a normal message into garbled form that cannot be read until it is converted back to readable text again. Authentication is a variation of the encryption process and ensures that the data sent has not been tampered with while en route to the receiver. This cryptographic issue will be discussed in more detail in Chapter VI.

4. Configuration management

A control must be established over program changes. The dynamic nature of business activities causes program changes in automated systems. Program changes require well-formulated and well-documented procedures to prevent the manipulation of programs for unauthorized purposes. Several procedures are necessary for maintaining control over program changes. [Ref. 7:p. 83]

- The nature of the proposed procedures change should be explained in writing , and formal approval for the change should be given by a responsible individual.
- Changes to the program should be done only by systems group, not operating group. And any change should be supported by adequate systems documentation. If the operator were authorized to make changes, it would greatly increase the difficulty of controlling manipulation and of maintaining up-to-date documentation.
- Changes should be tested and given final approval by a person who is separated from and independent of the person designing the change.
- The results should be recorded on program change registers, send to the responsible manager for approval. And then all change sheets, change registers, and printouts should be filed in program run book.

Data retention policies are also required in the electronic exchange of documents, as they are in paper-based systems. Duplicate copies of data files should be made with off-site storage. The data files should be logged and responsibility for physical custody should be appointed to someone not responsible for data entry, as discussed in the segment on the segregation of duties.

5. Documentation

The documentation of an internal electronic data processing application can be divided into three phases. These are data systems survey, data systems study, and programming. Consideration for internal control should be made in each phase. The data systems survey should outline the scope and objectives of application, the plan and schedule for completion, and estimated costs and benefits. An important control feature is approval by management before proceeding with the data systems study.

Data systems study should include a review of present procedures. This review should indicate what procedures and controls are necessary and beneficial in new system and what changes can be made in improving existing procedures. After a review of the present system, new or improved design should be done. During this phase, a documentation must be prepared for contents of master files, input/output requirements, methods of processing, estimated execution times, methods and timing of conversion, and so on. This documentation should be reviewed, approved, and signed by the responsible manager(s) concerned in order to ensure that these applications have been completely investigated, documented, and agreed upon before programming begins.

Computer programming is the preparation of flowcharts, program listings, and computer operating instructions. Such documentation is necessary to understand and control the programs as well as to provide a permanent history of all pertinent facts related to each program.

For efficient control for documentation, it is necessary that a standardization of procedures occur. These standards should be set up and maintained for convenience and

control efficiency. These standard should be contained in a written record of all policies, procedures, and techniques such as program documentation procedures, tape or disk labeling and retention policies, and program testing procedures. Well-practiced documentation standards contributes good control by preventing or reducing error(s) and for preventing manipulating by unauthorized personnel.

D. BACKUP AND DISASTER PLAN

For proper control purposes, procedures must exist to recover from the situations in which files are updated with incorrect data or inadvertently destroyed. These procedures should permit the recreation of a file with minimum effort; and the reconstruction plan must prohibit reuse of magnetic tapes or disks until the output from computer operations is proved correct and usable.

Generally, backup support for the files is accomplished by use of the grandfather-father-son concept. This concept is based on the fact that an organization usually produces an updated master file at each processing by reading the previous period's master file, making changes according to the transactions being processed, and writing the new file. [Ref. 7:p. 88] Hereby, the processing with tape or disk file should use a new tape or disk and does not destroy the old one. For example, if a certain file is updated daily, after processing of Wednesday's transactions, Monday's file should be grandfather-file, Tuesday's files should be father-file, and Wednesday's file should be son-file. If the files are to be recreated under the grandfather-father-son concept, the transaction files used to update the son file must be retained.

In addition, the contents of disk files should be duplicated on another machine-readable medium such as a tape or another disk so that the file can be reconstructed if the file is accidentally damaged or destroyed. The contents of disk files must be copied frequently enough to promptly recreate the destroyed master file. And in very long processing runs, test points and reprocessing procedures should be included to permit the computer operator to restart a program at an interim point in the processing rather having to return to the beginning of the run.

Internal controls also should be concerned with disaster events such as fire, floods, and blackouts, which will cause an organization's computer facilities to be out of operation for an extended period time. In order to cope with these disasters and to minimize processing problems, counterplans and arrangements should be made for use of backup facilities and alternative power sources. Also it is desirable to develop procedures to be followed in emergency conditions. An emergency plan should include a method to be used to process the current transactions to reconstruct any records that could be destroyed and to assign priorities to various processing jobs. In addition, insurance against such disasters is also useful control procedure which provides the organization with protection against financial loss.

E. AUDIT TRAIL

In any business information system, managers frequently need to detect and correct errors, and to substantiate that the system is processing information correctly. This substantiation is provided by the capability to track any transaction from origination to

closure. This physical tracking of a transaction through the system is made possible by an audit trail. The audit trail, also called a transaction trail, has been commonly defined as the accumulation of source documents and records that allows the organization to trace accounting entries back to their initiation and the reverse. It enables one to trace information in the financial statements and records back to the documents and also from the documents to the records and financial statements. When a system is computerized, source documents may be eliminated and data may be maintained only in machine-readable form. Furthermore, a computer has the ability to process transactions that accomplish several purposes simultaneously. Because of these characteristics, reports may be produced by a computer without a visible transaction trail that can be related to the individual transactions. In addition, this problem can be further complicated by summarization of the related details, which may eliminate data altogether. Therefore, a good audit trail is very important not only for effective internal control but also for external auditing.

For effectively establishing audit trail in an EDI environment, it may be helpful to investigate the major concerns posed by EDI. Several major issues regarding EDI that need to be resolved are: [Ref. 3:p. 47]

- As the physical documentation begins to disappear, the information once stored on those documents becomes more difficult for managers to segregate and retrieve. In effect, without proper auditing procedures and controls, responsible manager as decision makers may become somewhat removed from the decision making process.
- With introduction of EDI, data from day-to-day activities needs to be stored in electronic form. For some data, statutory requirements may dictate that data be

stored for a certain period of time. Electronic storage of data has the advantage of centralizing the data and actually permitting more and better controls over their operations. Methods of data storage should be planned before the implementation of EDI system.

- In the EDI environment, each functional department must supervise two separate and independent functions. For example, the purchasing department must supervise not only purchasing activities but also MIS applications that support it. This is certainly a difficult job. If proper control and supervision fails to occur, problems can arise. It is difficult to audit such an automated system using traditional inspection techniques. A great reliance is placed on the proper function of the system as well as the capabilities of individuals using the system.
- Increased potential for material errors because of reduced human involvement, uniformity of processing, unauthorized access, possibility loss of data.

Under these changing conditions in the electronic environment, several automated procedures must be developed with respect to providing an audit trail. These are: [Ref. 2:p. 43]

- Replace signatures with codes and IDs: The issues of such electronic signatures will be discussed in more detail in Chapter VI.
- Date/time stamp all automated activity and all attempts to access the information system.
- Maintain a specific audit trail database.
- Require identification of terminal/PC to track point of access.

In order to provide for good control and audit trail in an EDI environment, the above issues need to be carefully planned and implemented. As more trading partners and documents types are added to the EDI system, effective auditing and control procedures will need to be designed into the system. With effective planning, audit trailing and controlling the EDI is relatively painless. Some organizational and procedural elements will complement effective and proper audit trail and internal control of EDI system. These are:

- Well defined and clearly written job procedures.
- A systems user guide that parallels and complements the job procedures.
- Systems technical documentation.
- Professional functional users and MIS personnel.
- A well-run data center.

Since electronic data processing systems, involving EDI system, are very complicated, when these elements incorporated in totality, the overall control of EDI as well as establishing audit trail can significantly enhance the quality of EDI environment.

V. APPLICATION CONTROLS

A. INTRODUCTION

Application controls are designed to meet the specific control requirements of each processing application. This means that application controls are designed to ensure that EDI applications are processed accurately, completely, securely, and on a timely basis.

The objectives of application controls are to prevent, detect, or correct the various irregularities and anomalies in EDI applications. Because EDI is subject to various infringements, application control should be designed with the following objectives: [Ref. 7:p. 96]

- Assure that all authorized transactions are completely processed once and only once.
- Assure that transaction data are complete and accurate.
- Assure that transaction processing is correct and appropriate to the circumstances.
- Assure that processing results are utilized for the intended benefits.
- Assure that the application can continue to function.

In the EDI architecture, the communications interface and the EDI interface move electronic documents into and out of the application system. These automated processes replaced manual procedures such as keying in data. As a result, the control procedures in place for paper documents are no longer applicable. Application controls should exist at each processing stage to ensure transactions are moved through the communication interface completely and accurately, authorized appropriately, and sent to the correct application

system. Since the controls related to transactions are affected most by EDI implementation which is very complicated and technical, these transaction controls need to be modified and developed accordingly.

In this chapter, the completeness and accuracy of input controls as well as the authorization of transactions, and specific application control issues related to authorization of transactions will be discussed . These specific application control issues are authentication (user authentication), non-repudiation, and integrity (message authentication) in an EDI environment.

B. COMPLETENESS AND ACCURACY OF INPUT

Controls of completeness of input ensure that all transactions are input and accepted for processing once and only once. Typical techniques include checking documents sequentially as they are received, and batch totalling transactions as they are received and processed.[Ref. 1:p. 17] With respect to EDI, completeness of input controls should verify that all transactions sent by trading partner are passed and received by the appropriate application system. These controls should detect errors through each layer of EDI architecture.

In the communication interface layer, controls are needed to ensure that all transactions are transmitted from one computer system to another. Generally the techniques built into the communication software, such as check-bit testing, often provide adequate control. Typically, errors in transmissions are reported to the sender and transactions are re-transmitted.

Controls at the EDI interface layer are also needed to ensure that all transactions are passed through the EDI translator and application interface to the proper application system. As shown in the EDI data structures in Chapter II, new control techniques are designed that use data within the transaction - header or trailer for verification. Tracking control totals at transaction, functional group, or interchange level are common techniques used to ensure that all transactions are processed. Sequential control numbers assigned to each transmission by the sender or VAN can ensure that a transmission of multiple transactions is received completely.

During the EDI interface, error can result in the rejection of selected transactions or the entire transmission. Performing a match of the functional acknowledgements sent to the sending partner against transmission logs can help ensure that all transactions were received. Exception report, which records interrupted or rejected transmissions and other irregularities encountered during transmission, can help the auditor track erroneous transactions.

C. AUTHORIZATION OF TRANSACTION CONTROLS

Controls of authorization of transactions ensure that only valid and properly authorized transactions are processed. Generally, controls over authorization at the communications interface layer include general communication identification and sign-on procedures. However, at the EDI interface level, verification techniques are used in order to ensure that the sender is an approved trading partner and that the transactions sent are authorized for that partner. Codes such as customer numbers which are built into the transmission are commonly used.[Ref. 1:p. 19] Once an EDI relationship is established, trading partner's

customer number and authorized transactions may be maintained in a trading partner master file. Programmed procedures can check the validity of a partner and verify if partner is authorized to send a specific types of transaction. Any discrepancies found in exception reports can be verified against the master file or the legal trading partner agreement documentation.

Currently, as the use of EDI spreads into most business practices and the number of their trading partners increases, concerns about this transaction authorization process are increasing. These concerns are alleviated by techniques relating to authorization procedures such as passwords, authentication using testwords or electronic signatures, encryption, non-repudiation techniques, etc. These controls for authorization of transactions will be discussed in the following three parts separately. These are user authentication, non-repudiation, and integrity.

D. USER AUTHENTICATION

The primary management goals stress the timeliness and accuracy of all transactions. These goals cause EDI user to emphasize the use of authentication techniques, which protect against deliberate as well as accidental message alterations, rather than password or encryption entirely.

In the past, most systems have depended on manual controls to ensure that transactions are properly processed. These controls included matching various pieces of paper and reviewing previous documents for approval signature. For example, vendor invoices are generally matched to receiving reports and approved before payment in order

to assure that the goods and services have been received.

As most of current businesses are changing and developing toward highly automated systems, a business mechanism is needed that would allow a company to electronically transmit and process transaction or contractual information between the company and trading parties, perform electronic audits on the payment request for goods and services, and then electronically pay the resulting claim. This means that a current automated system require that it can be developed which can take electronic information from several different sources and authorize a payment or other action without the familiar hand written signature and paper document.

The answer for this is the authentication techniques. Authentication scheme can help ensure authorization, especially in the absence of manual approval procedures. Authentication entails the use of a secret password or an electronic signature that is built into the transaction set, functional group, or interchange to verify the identity of the originator.

VANs provide authentication services. Several techniques for authentication are also available currently. One good technique for authentication is the use of electronic signatures with the cryptographic method. These techniques for authentication will be discussed in detail in Chapter VI. Technical parts regarding to electronic signatures in Chapter VI are related not only to authentication but also to non-repudiation and integrity which will be discussed subsequently in this chapter.

E. NON-REPUDIATION

Under EDI environment, one of the big control issues is the repudiation problem. In the previous paper-based systems, it did not pose a control problem because paper itself is critical evidence for transactions or contract. However, since EDI is a paperless system in which all documents are transmitted not only between most internal departments in the company but, especially, between the company and external trading partners, then, it could lead to severe problems if control is not exercised. Furthermore, it might be also lead to serious legal issues between a company and the dishonest trading partner.

For example, suppose that the company buys a thousand ton of law material for his trading partner's order, and immediately thereafter the price of that law material's price drops sharply. A dishonest trading partner might sue the company, claiming that he never issued any order to buy the law material. When the company produce the message in court, the customer can deny having sent it. The company must prove in court that the message was received from that trading partner. How should the company deal with this repudiation internal control problem?

Authentication and non-repudiation is very critical issue of internal control that should be controlled without fail under automated environment. In an EDI environment, if a company is using the VAN, the company can gain the non-repudiation service. These are: [Ref. 10:p. 34]

- Non-repudiation of content originated: This element of service enables the originating EDI user agency (sender) to provide a recipient EDI user agency (receiver) with an irrevocable proof as to the authentication and integrity of the

content of the message.

- Non-repudiation of content received: This element of service enables an originating EDI user agency to get from a recipient EDI user agency an irrevocable proof that the original subject message content was received by the recipient EDI user agency and EDI message responsibility was accepted, forwarded or refused. It will protect against any attempt by the recipient(s) to subsequently deny having received the message content. This service is stronger than the proof of content received service.

In addition, fortunately, this repudiation problem also can be resolved without using a VAN facility. Currently cryptographic methods are available and are very useful to solve the repudiation control problems. These are methods that use digital signatures with public key cryptography or conventional cryptography. These methods also can be used to control the authentication and integrity in an EDI environment. These methods will be discussed in detail in the next chapter.

F. INTEGRITY: MESSAGE AUTHENTICATION

When an auditor reviews a system, one question that must be answered is how the system ensures data integrity. In paper-based environment, this is relatively easy process -- just look at a piece of paper. A totally automated process, however, requires far more skills and sophisticated methods to provide the same degree of assurance. In these fully automated systems, if internal controls are not well-formulated and not well-performed, it allows a knowledgeable perpetrator to access, modify, or destroy the company's computer

data, programs, and other resources without leaving any audit trail. Especially, since EDI system is paperless system in which data or documents are transmitted via uncontrollable lines, these weakness could be increased. Although use of VAN services reduces such weaknesses, its vulnerabilities still remain. Thus data or documents transmitted electronically must be controlled. This protection method of data or documents is message authentication.

The traditional message authentication techniques are methods called testwords or test keys. A typical testword system creates an authentication code using as an input the transaction value, the date, a sequence number (not used by all institutions), and/or a random number. Testword systems may provide a redundancy check on the amount field and, when sequence number is used, provide information on missing or duplicate transactions. With advent of computers, the testword algorithms become more sophisticated and a lot of bank in the world has used them for their user's authentication.[Ref. 8:p. 342]

Such a family of authentication method, testwords or test keys method, were perfectly adequate for earlier authentic activity. However, they look much less adequate in the current environment where there is an absence of voice recognition, most of the assets flow with no intervention, and there is widespread availability of microcomputers as tools for potential criminals.

Because testword systems neither provided the requisite security nor transaction processing growth potential for the future, a message authentication standard was developed. This standard, X9.9 - 1982, financial institution message authentication, utilizes the Data Encryption Algorithm(DEA) and a secret key to derive a checksum called a Message Authentication Code(MAC) from the financial message.

DEA was chosen initially as the algorithm because there was no public key algorithm available. DEA continues to be the algorithm of choice for authentication, encryption, and key management for several reasons. These are:

- There is no national or international standard public key algorithm; use of an algorithm other than DEA could be considered imprudent business practice.
- All available public key algorithms require a secure, initial distribution of variables such as networks.
- There are a variety of DEA chips available currently - at varying speeds and with differing operational characteristics.

Authentication is designed to be an end-to-end process, in the sense that a new MAC must be computed using a unique key by any parties to the transaction that modifies the message. Such modification carries with it the assumption of financial or legal liabilities for the changed transaction. Currently, authentication procedures using both the public and private together are also available by using cryptographic methods for a certain field of documents or for the entire document. These technical methods of message authentication and encryption will be discussed in Chapter VI.

VI. LEGAL ISSUES

Currently, the use of EDI is increasing significantly in various businesses. Several factors have contributed to the expanding popularity of EDI systems: these are the relatively low cost of EDI software and hardware, a developed set of standards for communication, and an increasing use of just-in-time(JIT) manufacturing and purchasing techniques. Such increased use of EDI, however, has led to a reduction in the paper evidence of transactions both sent and received. This loss of a paper audit trail in an EDI environment gives rise to potentially serious legal issues. As the use of EDI increases, these issues are highlighted not only between trading parties, but also in EDI organizations as a whole. Most of the firms that participated in the EDI survey[Ref. 12:p. 81-86] thought that this might be a major obstacle to the implementation of an EDI system. In fact, current technology is progressing at a faster pace than law. It is apparent that there will be both legal and policy impediments to rapid implementation of EDI technologies. Two major legal issues which will be discussed in this chapter are trading partner agreements and electronic signature.

A. TRADING PARTNER AGREEMENTS

Currently, legal issues are being addressed primarily in written trading partner agreements that serve as contracts between trading parties. General contract law allows contracting parties to dictate the terms of their participation in a contract. Trading partner agreements manifest the terms of the contractual relationship and authorized EDI transactions and assign responsibilities in the event of problems or conflicts.

Trading partner agreements are the most common means of establishing a legal platform between partners. In other words, the agreement specifies the conditions under which certain trading partners will exchange business information electronically. With documents being sent electronically, contract terms and conditions will no longer be sent to trading partners with each transaction. Before beginning transactions between two parties, or during the transactions, a blanket trading partner agreement is prepared and signed. Then it is considered valid for all EDI transactions.

Generally, trading partner agreements can include several items such as payment term, liability, need for acknowledgements, communication charge and so on.[Ref.2: p. 46]

- Payment terms: It may stipulate that payments be made through EDI/EFT.
- Liability: Who is responsible for a specific issue such as transmission error?
- Need for acknowledgements: EDI provides for instantaneous acknowledgements that serve as "signed receipt requested" letter.
- Communication charge: Will a VAN be used? What documents will be sent or received through EDI? Who pays data transmission bill?

For example, in EDI trading partner agreement for defence transportation, the main text of the agreement presents general guideline for all EDI applications such as purpose, reference, objective, scope, definition of additional terms, force majeure, effective date, express agreement review, termination, disputes and whole agreement. The addenda to the agreement provide detailed guidance for exchanging information contained in specific documents. Appendix A shows an example of trading partner agreements for defense transportation.[Ref. 11: p. 1-4]

These trading partner agreements have a very important role in implementing EDI as they give protection to both trading partners. These agreement are company specific and therefore may or may not be directly applicable to other firms in particular situations. It is clear that trading partners must have a specific agreement signed by both themselves and trading partner before EDI transmissions begin. Each EDI firm should obtain the help and advice of legal counsel prior to operationalizing EDI.

B. ELECTRONIC SIGNATURE

1. Introduction

In an EDI system, no paper is transferred between companies and their trading partners, and most of the documents are transmitted or communicated through VAN. For computerized message systems to replace the physical transport of paper and ink documents, a solution must be found to the authentication problem because the electronic transmission of documents can not be authenticated by the conventional signature. Also a solution must be found to the information security problem because documents are often transmitted across a public network.

However, the problem of devising a replacement for handwritten signature is a difficult one. Basically what is needed is a system by which one party can send a signed message to another party in such way that the receiver can verify the claimed identity of sender and that the sender cannot later repudiate the message.

The traditional approach is to have a user prove his identity by typing in a password. Not only does this method expose the user to passive wiretapping, but also it may require

the authenticating computer to maintain a list of password internally, which is itself a potential security problem.

Fortunately, technology called electronic signature, using cryptographic processes, is being introduced in an EDI environment. An electronic signature is a symbol, generated through electronic means, that can be used to validate the sender's identity and the integrity of the critical information received from the sender. The objectives of an electronic signature are ultimately secret and authentication of data transmission between trading partners.

Diffie and Hellman's article(1976) introduced the new cryptography method, which caused a basic revolution in the way people think about cryptographic system. This method was to use an encryption algorithm, E, and a decryption algorithm, D, with E and D chosen so that deriving D even given a complete description of E would be effectively impossible. There are three requirements here: [Ref. 6:p. 514]

- D (E (P)) = P: If we apply D to an encrypted message, E(P), we get the original plaintext message, P, back.
- It is exceedingly difficult to deduce D from E.
- E can not be broken by a chosen plaintext attack: It is needed because intruders may experiment with the algorithm to their heart's content.

Under such conditions, there is no reason that E can not be made public. Any person or organization wanting to receive secret messages first devises two algorithm, E and D, meeting the above requirements. The encryption algorithm or key made public. This method is called "public key cryptography". This might be done by putting it in a file that anyone

who wanted to could read.

For example, when opening an account in a certain bank, a customer chooses a public key and a private key. He/she gives the public key to the bank and keeps the private key himself/herself. When the customer calls the bank to establish a session, the bank chooses a random number, encodes it with the alleged customer's public key, and challenges the caller to send it back unencrypted. (The message encrypted by the public key can only be decrypted by its corresponding private key.) Only person knowing the decryption key is able to perform the decryption, so impostors will fail the test. Also, an intruder recording all the traffic will have no benefit because next time the bank will choose a different random number. For additional security, the bank might require its customers to include in each message a secret password, a sequence number, the time and date of transmission, and a checksum of the entire plaintext including the time, date, and sequence number. The sequence number makes it pointless for intruder to record and subsequently play back the message, because the bank can see that they are just duplicates of earlier messages. The time and date makes it useless for the intruder to save a record message until the sequence numbers have cycled around. The checksum makes it highly improbable that an intruder could forge or modify a (ciphertext) message and still have the (plaintext) checksum be correct.[Ref. 6:p. 517]

There is one of good algorithm which was discovered by a group at MIT. Their cryptographic algorithm method is based on some principles from number theory. The way to use the method is shown below.

1. Choose two large primes, p and q, each greater than 10^{100}.

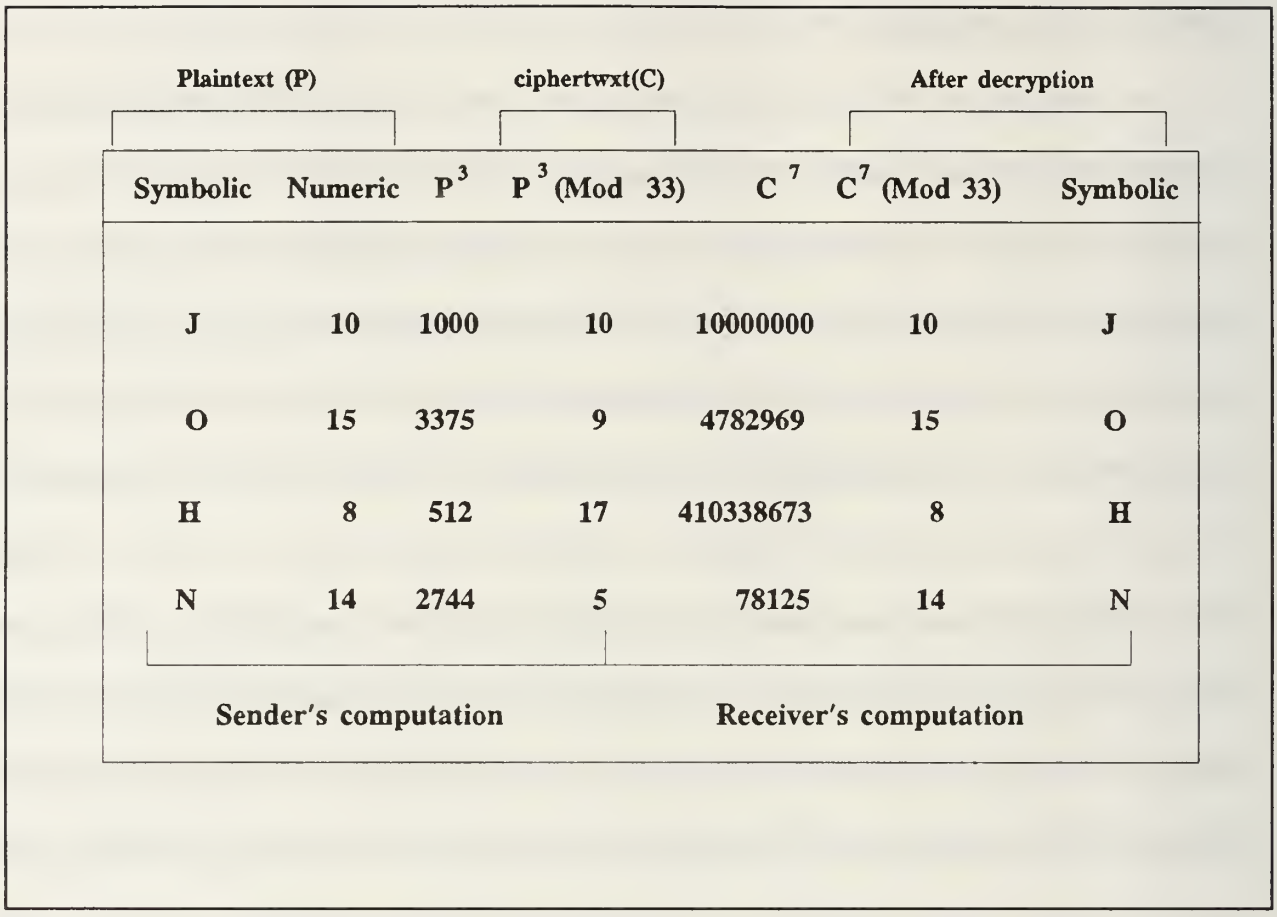

Figure 11 An example of the MIT algorithm.

2. Compute n = p × q and z = (p-1) × (q-1).

3. Choose a number relatively prime to z and call it d.

4. Find e such that e × d = 1 mode z.

A simple pedagogical example of MIT algorithm is given in Figure 11. For this example we have chosen p=3 and q=11, giving n=33 and z=20. A suitable value for d is d=7, because 7 and 20 have no common factors. With these choices, e can be found by solving the equation 7e=1 (mod 20), which yields e=3. The ciphertext, C, for a plaintext message, P, is given by $C=P^3$ (mod 33). The ciphertext is decrypted by receiver according to the rule $P=C^7$ (mod 33). The figure shows the encryption of plaintext "JOHN" as an

example. Because the primes chosen for this example are so small, P must be less than 33, so each plaintext block can contain only a single character. The result is a monoalphabetic substitution cipher, not very impressive. If what we had chosen for p and q were approximately 10^{100}, n would be 10^{200}, so each block could be up to 664 bits ($2^{664} \approx 10^{200}$) or 83 8-bit characters.

2. Digital signatures with public key cryptography

In using the electronic transmission of documents, an electronic signature is necessary not only to verify the claimed identity of the sender but also to prevent the original sender's from later repudiating the message. Even though an EDI company uses an encryption and authentication method in secure electronic data transfer between companies, there are still the problems of preventing dishonest customers from repudiating their previous messages. Under certain conditions, public key cryptography can make an important contribution to solving this problem. To use public key cryptography for sending signed messages, it is necessary that the encryption algorithm E and the decryption algorithm D have the property that E(D(P)) = P. Suppose that A sends a signed plaintext message P to B by transmitting $E_B(D_A(P))$. A knows his own secret decryption key, D_A, as well as the public key of B, E_B. When B receives the message, he transforms it using his private key, yielding $D_A(P)$. He stores this text in a safe place and then decrypts it using E_A to get the original plaintext.

In order to see how the signature property works, assume that A subsequently denies having sent the message P to B. When the case comes up in court, B can produce both P and $D_A(P)$. The judge can easily verify that B indeed has a valid message encrypted by D_A by simply applying E_A to it. Because B cannot know what secret key of A is, the only way

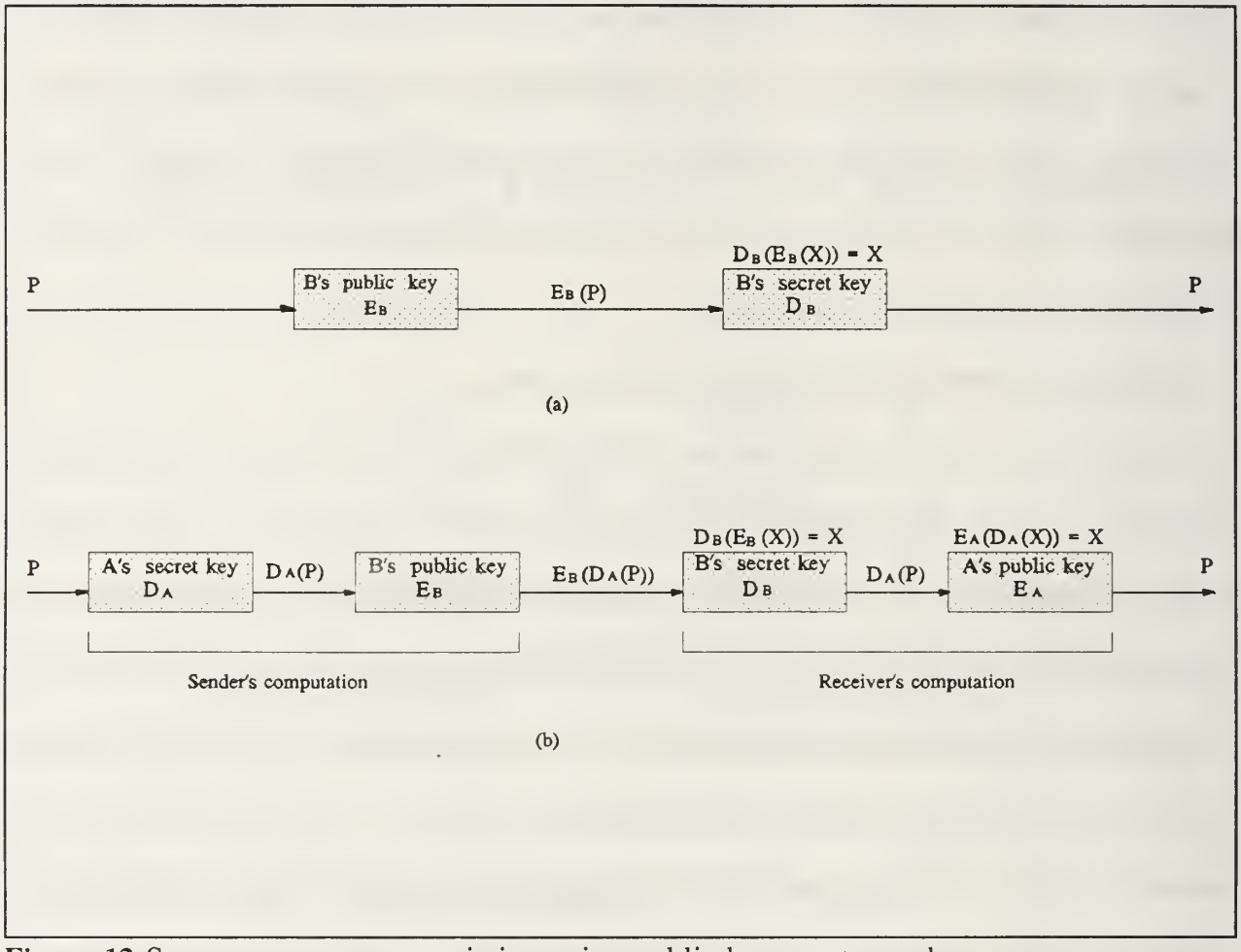

Figure 12 Secure message transmission using public key cryptography

B could have acquired a message encrypted by it is if A indeed sent it. Figure 12 illustrates a secure message transmission using public key cryptography including (a) without signature and (b) with signature.[Ref. 6:p. 518]

One criticism of this signature method is that it couples two distinct functions: authentication and secrecy. In many applications, authentication is essential but secrecy is not. Because public key cryptography is slow, it is frequently desirable to be able to send signed plaintext documents. The following description is an authentication scheme that does not require encrypting the entire message.

This authentication mechanism is based on the idea of one-way checksum function, CK. given a plaintext message, P, it must be relatively easy to calculate CK(P), but given CK(P) it must be nearly impossible to find a P that yields this checksum. The checksum, CK(P), should be smaller than the message. Many mathematical functions with this one-way property exist. To sign a plaintext message(P), the sender(A) first computes CK(P) and then applies his private key to it, to yield $D_A(CK(P))$. He then transmits the pair[P,$D_A(CK(P))$] to B.

When everything arrives, B applies E_A to the signature part to yield CK(P). At this point B holds three items: P, CK(P), and $D_A(CK(P))$. B now applies CK to P to see if the checksum so computed agrees with checksum received along with the message. Then, he knows that the message has not been tampered with. If the checksum disagrees, the message has been forged. When the problem of repudiating a previous message by dishonest customer occurs(A), B can show all three items to a judge to prove that A did indeed send the message. Obviously, the judge knows that even if B fabricated P and CK(P), there is no way B could have computed $D_A(CK(P))$ without access to A's private key. The merit of this scheme is that only the short checksum has to undergo the expensive public key encryption, no matter how long the message is. In contrast, if it were possible to find a plaintext message P that corresponded to CK(P), then B could cheat by generating a new message, P´, the with same checksum as P and show P´,CK(P), and $D_A(CK(P))$ to the judge.

However, both of these signature methods have some problems related to the environment in which they operate rather than with the algorithms themselves. For one thing, B can prove that a message was sent by A only as long as D_A remains secret. If A

discloses his secret key, anyone could have sent the message,including B. Another problem is what happens if A decides to change his key. Doing so is clearly legal and may even be standard operating procedure within many companies. If a court case later arises, the judge will apply the current E_A to $D_A(P)$ or $D_A(CK(P))$ and discover that it does not produce P or CK(P), respectively. At this time, B may have a problem to prove it. Consequently, it appears that some central authority is required to record all key changes and their dates.

3. Digital signatures with conventional cryptography

By having a central authority, say C, both secrecy and electronic digital signature can be obtained using conventional cryptography. One way to get secrecy is to require each user to choose and hand-carry it to C's office. Therefore, only A and C know A's secret key, K_A. If A wants to communicate or transmit a document, A can ask C to choose a session key, K_S, and send him two copies of it, one encrypted with K_A, and one encrypted with K_B. A then sends the latter to B with instructions to decrypt it using K_B and then plaintext as the session key. If users want to send signed one, C can also provide a signature service using a special key, X, keep secret from everyone. In order to use the signature service, the following procedures are progressed.[Ref.6:p. 520]

- A, say customer, sends $K_A(P)$ to C, central authority.
- C decrypts $K_A(P)$ to get P, then build a new message consisting of A's name and address concatenated with the date, D, and the original message. This new message, A + D + P, is then encrypted with X, yielding X(A + D + P) and send back to A. C can verify that the request indeed came from A, because only A and C know K_A. An intruder would not be able to send C a message that made sense when decrypted

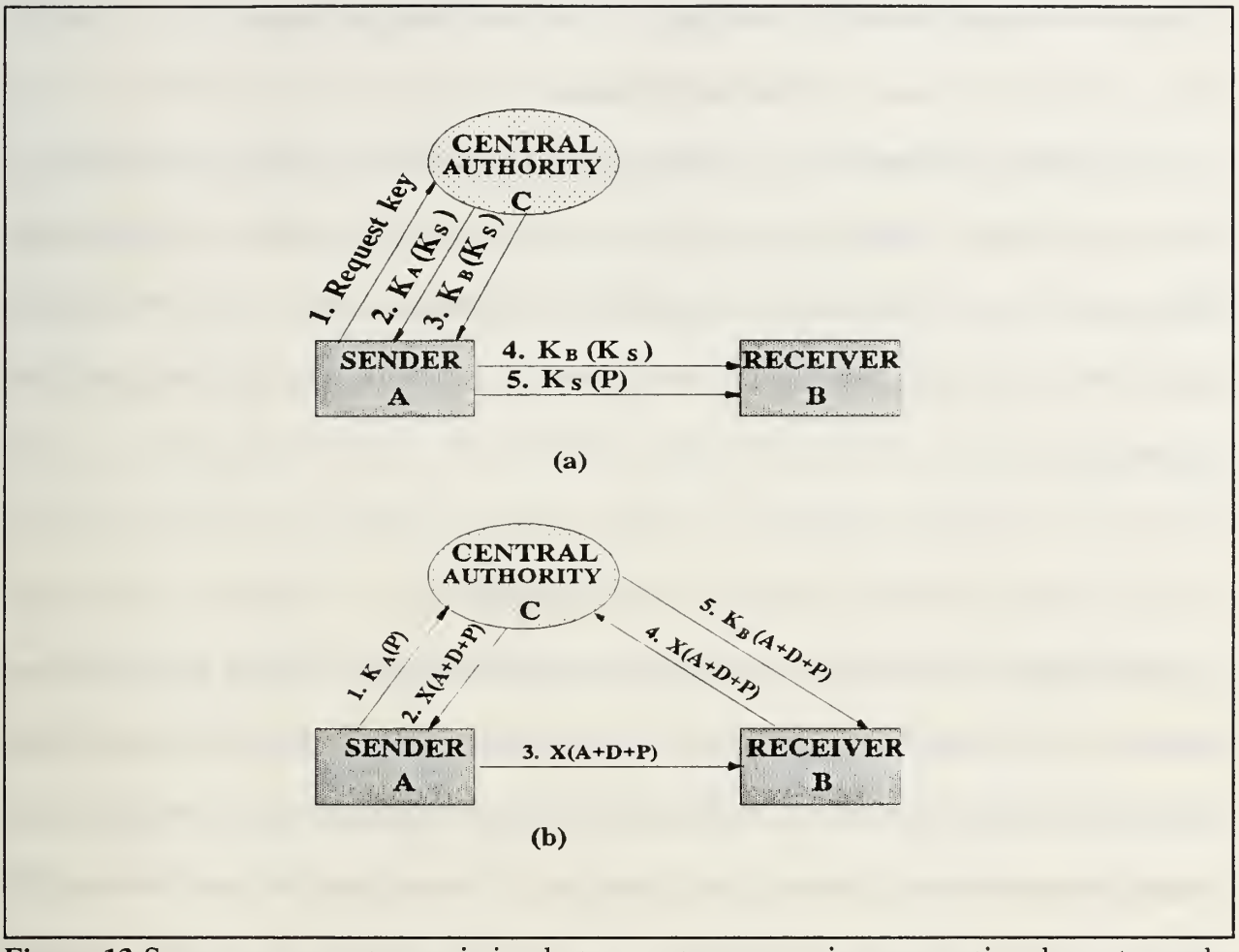

Figure 13 Secure message transmission between strangers using conventional cryptography

by K_A. The ability of C to authenticate A is the heart of the signature mechanism.

- A sends X(A + D + P) to B, say a bank.
- B, the bank, sends X(A + D + P) to C, requesting K_B(A + D + P) as a result.
- The bank then decrypts K_B(A + D + P) to recover the plaintext information A, D, and P.

Figure 13 illustrates the secure message transmission between total strangers using conventional cryptography.[Ref. 6:p. 521] When the signatures are not needed, as in Figure 13(a), after the session key has been established by steps 1, 2, 3, 4 and 5, central authority,

C, must be no longer needed. In contrast, in the signed message transmission as in Figure 13(b), C must be invoked twice for each message.

If A denies sending P to B, B can show X(A + D + P) to a judge. The judge then order C to decrypt it. When the judge sees A, D, and P, he knows that A is lying, because B does not know X, and therefore could not have fabricated X(A + D + P). But, the problem of A's claiming that his K_A was stolen still exist, just as in previous public key cryptography.

C. EDI AND LAW OF CONTRACT FORMATION

The English "Act of the Prevention of Fraud and Perjuries" of 1677, which has been adopted in state contract laws and known as the statute of frauds, prescribes the prohibition on the juridical enforcement of most executory contracts unless they are evidenced by some note or memorandum in writing signed by the parties to be charged by such contract. This statute was intended not only to obviate perjury, but also to lessen the need for juridical reliance on verbal evidence. For this purpose, it adopted the most advanced data transmission and storage technology available at the time, paper and ink.[Ref. 9:p. 1]

However, the technology which will permit two parties to enter into a contract through the use of EDI, eliminating the paper and signature, is being developed rapidly in most business area. Also the use of confidential codes, encryption, or other security technologies will provide the parties to an electronic transaction with the requisite assurances that they are not dealing with an impostor and that the data being exchanged are authentic, in essence an electronic signature. Furthermore, the contractual relationship can be defined

through the use of trading partner agreements by which parties settle in advance on the general conditions which will govern their future transactions.

In these circumstances, the question arises whether the statute of frauds has become an outdated and unnecessary impediment to contract formation in the emerging paperless environment. In the context of private contracting, even in the public sector, suggestions have been made that the time may be ripe to abolish the statue of frauds for the sales of goods or, less radically, that it be modified to explicitly state when and how electronic communications may constitute a signed writing or to sanction explicitly some form of appropriate authentication technology.

A series of judicial precedents relating to these issue indicates that if a certain party does not fulfil the recordation requirements, it can neither automatically take the benefit of an agreement it has allegedly made, nor can it be hurt by another alleging an agreement. This means that it still requires that the contract be supported by documentary evidence of a binding agreement in writing. Exceptions are allowed, however, when an implied-in-fact contract is found.

Therefore, companies which entered into contract electronically should be able to prove that the parties entered an implied-in-fact contract. Extensive negotiations in which the parties demonstrate hope and intent to reach an agreement are not sufficient in themselves to establish a contract implied-in-fact. This agreement of implied in fact is based on the meeting of minds. Even though it is not embodied in an express contract, it can be inferred from conduct of the parties showing in the light of the surrounding circumstances their tacit understanding. In order for an implied in fact contract to be found, a party must show each

element of a contract, including meeting of minds, consideration,etc. An EDI system can no doubt be structured in such a way that a party to a transaction can retrieve the information essential to the making of the requisite factual showing. Since the parties to such an electronic contract would clearly not be contemplating a written agreement in the traditional sense, the courts would likely not hesitate to find an implied in fact contract.

Currently, some contend to abolish the statute's requirement. And there is also a view that these information storage and retrieval technologies can be made just as reliable as paper and ink, and constitute writing in fact if not in law.[Ref. 9:p. 12] In the text of private sector contracting, U.C.C. section 1-201(46) provides that a "· · · writing includes printing, typewriting or any other reduction to tangible form." This language can be construed to include the outputs of EDI technologies.

VII. CONCLUSION

Generally, EDI provides significant advantages for most business, involving increased productivity, improved customer services and heightened ability to compete in the international marketplace. The reduction in paper-work, timely communication flow, and greater accuracy of data are more direct benefits of EDI. However, these benefits that result from paper substitution can be negated if the environment is not controlled and security is not maintained properly. Internal controls, both general and application, need to be reviewed, and often modified to encompass risks that are concomitant with the use of EDI.

From the point of view of the information systems manager, an EDI project, as another major computer application, is also subject to the policies, procedures, and controls of systems development life cycle. Controls over EDI systems are essential to ensure the integrity of transactions and their data, and to enable users to drive maximum benefits. Some control requirements are unique to the EDI system. Others are existing procedures that need to be re-evaluated when new technology is introduced into the environment.[Ref. 1:p. 24] EDI is unusual in that it may impact a variety of applications already in existence, such as purchasing, sales order processing and production scheduling. Integration of EDI into these functions may entail significant system modifications.

EDI development, like any other application system, requires a thorough planning, extensive user involvement, feasibility studies, and design specifications that build in the necessary controls -- audit trail, backup and recovery procedures, and security considerations. An EDI system also requires continuing maintenance as communication

standards evolve and network partners are added and deleted. Besides, EDI development requires more and more sophisticated techniques to keep up with the changing technological environment. Some examples are the availability of cryptographic method for authentication, integrity of message, and non-repudiation.

There are several legal issues relating to implementation of EDI, because of paper reduction and less human intervention. These are electronic signature for authentication, integrity of messages and non-repudiation, and law of contractual formation, etc. In order to alleviate potential problems due to vulnerability of these legal issues, trading partner agreements which define the terms of the EDI relationship should be developed between trading parties before transactions begin. File retention is important, as is the generation of acknowledgements by the system as a substantiation of business conducted.

In conclusion, as the use of EDI increases through interface with more in-house applications and the inclusion of more and more trading partners, the importance of EDI to overall company stability and growth will continue to expand. In addition, it will provide competitive and strategic advantages to EDI company continuously. Although significant benefits can be derived from the use of EDI system, those benefits for the use of EDI can be feasible only when internal controls through EDI company whole conduct effectively and systematically.

APPENDIX. A

ELECTRONIC DATA INTERCHANGE TRADING PARTNER AGREEMENT FOR DEFENSE TRANSPORTATION

1. **Purpose:** This agreement prescribes the general procedures and policies to be followed by DoD activities when using electronic data interchange (EDI) techniques for transmitting and receiving tender, shipment, billing, or other transportation information. Several addenda provide additional detail on the policies and procedures for transmitting specific business information electronically.

The purpose of this agreement is to ensure that all EDI-created obligations are legally binding on all trading partners. It also is an agreement that any electronic equivalent of the documents referenced in Paragraph 2 below will be deemed an acceptable business practice and that no trading partner will challenge the admissibility of the electronic information in evidence except in circumstances in which an analogous paper document could be challenged.

2. **Reference:** This agreement is subject to the terms and conditions of the following documents, which are hereby incorporated by reference:

- Government Bills of Lading (GBLs), Standard Form (SF) 1103
- Public Voucher, SF 1113
- Title 41, Code of Federal Regulations (CFR)
- Defense Traffic Management Regulations[1]
  - AR 55-355
  - NAVSUPINST 4600.70
  - AFR 75-2
  - MCO P4600.14B
  - DLAR 4500.3

[1]Army Regulation (AR), Naval Supply System Command Instruction (NAVSUPINST), Air Force Regulation (AFR), Marine Corps Ordnance Publication (MCO), and Defense Logistics Agency Regulation (DLAR).

- Department of Defense Standard Tender of Freight Services, SF 364-R
- Instructions for Use, DoD Standard Tender of Freight Services
- Uniform Tender of Rates and/or Charges for Transportation Services, Optional Form 280
- MTMC[2] Freight Traffic Rules Publication No. 1 (Motor)
- MTMC Freight Traffic Rules Publication No. 10 (Rail)
- MTMC Class Rate Publication No. 100.

3. **Objective:** The DoD expressly desires to maximize its use of EDI when purchasing and/or paying for freight services for the account of the United States.

4. **Scope:** Information exchanged through EDI will be the same as that currently required on the paper documents. The required signature or signatures will be electronically transmitted using a discrete authenticating code described in each transaction set addendum. This agreement binds the signatories to all the requirements of the documents referenced in Paragraph 2 with the exception of the forms being used.

5. **Additional Terms:** The following additional terms are made part of this agreement:

- MTMC, DoD shippers, and DoD finance centers will adhere to published American National Standards Institute (ANSI) X12 and Transportation Data Coordination Committee (TDCC) standards for approved transaction sets and will comply with DoD and industry implementation guidelines unless otherwise agreed to by all trading partners.
- MTMC, DoD shippers, and DoD finance centers will support the current and previous versions of ANSI X12 and TDCC standards. They will give all trading partners at least 90 days' notice of an intent to upgrade to a new published ANSI X12 or TDCC standard. The trading partners will then change to the upgraded standards within 180 days of the date of conversion published by MTMC, DoD shippers, or DoD finance centers or within 180 days of the actual conversion date, whichever is later. MTMC, DoD shippers, and DoD finance centers will discontinue support of the previous version of the standard within 30 days of the trading partner conversion date or 180 days after that conversion, whichever is later.

---

[2]Military Traffic Management Command.

- When initiating a new electronic trading relationship, all parties will engage in a parallel test until they are satisfied with the integrity of the electronically transmitted data.
- The recipient of EDI communications will use reasonable automated procedures to check the transmissions for compliance with ANSI X12 and/or TDCC syntax and format standards and for lost or altered data. If the recipient finds errors in compliance or if data are lost or altered, the recipient will so inform the originator with an appropriate functional acknowledgment transaction set or by telephone within 24 hours. The recipient will not be required to take any further steps to test for mistakes, fraud, or unauthorized transmission.
- MTMC, DoD shippers, and DoD finance centers will exchange business data with carriers through third-party networks described in the individual transaction set addenda. The originator of any EDI transmission will be responsible for third-party network charges unless previously agreed upon or otherwise specified in the addendum. The carriers will be responsible for their hardware and software costs associated with EDI.
- All parties will review and collect the contents of their mailboxes at the times described within each transaction set addendum. All messages will be deemed received and legally binding when the recipient actually collects its mailbox contents or at the time the recipient is required to collect its mailbox contents under the terms of this agreement, whichever is earlier.
- A functional acknowledgment, ANSI X12 Transaction Set 997, will be transmitted, by agreement of the EDI trading partners. A carrier that elects not to receive the functional acknowledgment will be responsible for using whatever means it wishes to ensure that the EDI message was received.

6. **Force Majeure**: No party to this agreement will be liable for failure to properly conduct EDI in the event of war; accident; riot; fire; explosion; flood; epidemic; power outage; labor dispute; act of God; act of Government; act of public enemy; malfunction or inappropriate design of hardware or software; error of, or nonperformance by, a third-party network; or any other cause beyond such party's control.

7. **Effective Date**: The effective date of this agreement will be the last signed date shown on the signature page of this agreement. The effective date of any addendum, if later than this agreement, will be governed by Paragraph 11 below.

8. **Express Agreement Review**: This agreement will be reviewed annually by the trading partners to make the changes, additions, or deletions that may be required.

9. Termination: This agreement may be terminated by either MTMC or the carrier effective 30 days after written notice by either party. It also may be terminated by MTMC if the carrier's EDI performance level is unacceptable and the carrier does not correct that performance after notification. Termination will have no effect on transactions occurring prior to the effective date of termination.

10. Disputes: All disputes, differences or disagreements, and/or claims between the parties arising out of this agreement that are not resolved by negotiation shall be subject to and adjudicated according to the procedures in 41 CFR 101-41.5, "Claims by the United States Relating to Transportation Services"; 41 CFR 101-41.6, "Claims Against the United States Relating to Transportation Services"; and 41 CFR 101-41.7, "Reconsideration and Review of General Services Administration Transportation Claims Settlements."

11. Whole Agreement: This agreement and all addenda constitute the entire agreement between the parties. No change in the terms and conditions of this agreement shall be effective unless approved in writing and signed by both parties hereto. At the inception of this agreement, Addendum/Addenda _____ (A, B, C, D) (is) (are) applicable. As the parties develop and implement additional EDI capabilities, addenda may be incorporated into this agreement. Each addendum will be signed by the parties and dated. The date of the last signature will be the effective date. The addenda will be appended to this agreement.

(seal)	(seal)
_____	_____
Representing:	Representing MTMC
_____	_____
_____	_____
Typed name and title	Typed name and title
Date: _____	Date: _____

REFERENCES

1. William J. Powers, *EDI Control and Audit Issues*, 1989.

2. Kathleen Conlon Hinge, *Electronic data Interchange*, AMA Membership Publications Divisions, 1988.

3. Robert M. Monczka and Joseph R. Carter, *Electronic Data Interchange: Managing Implementation in a Purchasing Environment*, Sponsored by the Computer Information System, 1989.

4. M. Emmelhainz, *Electronic Data Interchange: A Total Management Guide*, Van Nostrand Reinhold, 1989.

5. John Burch, *The Case of The Reluctant EDIer*, Journal of Systems Management, Mar 1989.

6. Andrew S. Tanenbaum, *Computer Networks*, Prentice Hall, 1988.

7. W. Thomas Porter and William E. Perry, *EDP: Controls and Auditing,* Kent Publishing Company, 1985.

8. Alvin A. Arens and James K. Loebbecke, *Auditing: An Integrated Approach,* Prentice Hall, 1988.

9. Peter N. Weiss, *EDI and the Law of Public Contract Formation: Will the Federal "Statute of Frauds" Thwart the Paperless Contract?,* 1990.

10. *Message Handling: EDI Messaging Service,* CCITT The International Telegraph and Telephone Consultative Committee, Jun 1990.

11. Ben W. Milbrandt and John A. Ciucci, *EDI Trading Partner Agreement for Defense Transportation,* Logistics Management Institute, Jan 1990.

12. *EDI,* Computerworld, 26 Mar 1990.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center — 2
   Cameron Station
   Alexandria, VA 22304-6145

2. Library, Code 052 — 2
   Naval Postgraduate School
   Monterey, CA 93943-5002

3. Professor Myung W. Suh — 2
   Code AS/SU
   Naval Postgraduate School
   Monterey, CA 93943-5000

4. Professor Shu S. Liao — 1
   Code AS/LC
   Naval Postgraduate School
   Monterey, CA 93943-5000

5. Library, P.O. Box 77 — 1
   Gong Neung Dong, Dobong Gu
   Seoul, Republic of Korea

6. Bae, Dal Hyeoung 5

Deagu City, Dong Gu Yong-su Dong 624,

Republic of Korea